



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ :

H04M 7/00, 3/48, H04L 12/64, 29/06

A3

(11) International Publication Number:

WO 98/34391

(43) International Publication Date:

6 August 1998 (06.08.98)

(21) International Application Number: PCT/US98/01868

(22) International Filing Date: 3 February 1998 (03.02.98)

(30) Priority Data:

08/794,555	3 February 1997 (03.02.97)	US
08/794,114	3 February 1997 (03.02.97)	US
08/794,689	3 February 1997 (03.02.97)	US
08/807,130	10 February 1997 (10.02.97)	US
08/798,208	10 February 1997 (10.02.97)	US
08/795,270	10 February 1997 (10.02.97)	US
08/797,964	10 February 1997 (10.02.97)	US
08/800,243	10 February 1997 (10.02.97)	US
08/798,350	10 February 1997 (10.02.97)	US
08/797,445	10 February 1997 (10.02.97)	US
08/797,360	10 February 1997 (10.02.97)	US

(71) Applicant: MCI COMMUNICATIONS CORPORATION
[US/US]; 1133 19th Street, N.W., Washington, DC 20036
(US).

(71)(72) Applicants and Inventors: EASTEP, Guido, M. [US/US]; 3005 Saint Germain Road, McKinney, TX 75070 (US). LITZENBERGER, Paul, R. [US/US]; 320 West Oak Street, Wylie, TX 75098 (US). OREBAUGH, Shannon, R. [US/US]; 12588 Rock Ridge Road, Herndon, VA 20170 (US). ELLIOTT, Isaac, K. [US/US]; 3855 Orchard Drive, Colorado Springs, CO 80920 (US). STELLE, Rick [US/US]; 6314 Dewsbury Drive, Colorado Springs, CO 80918 (US). SCHRAGE, Bruce [US/US]; 6560 W. Gambol Quail Drive, Colorado Springs, CO 80918 (US). BAXTER, Craig, A. [US/US]; 8495 Vance Court, Colorado Springs, CO 80919 (US). ATKINSON, Wesley [US/US]; 22 Morning Star Circle, Woodland Park, CO 80863 (US). KNOSTMAN, Chuck [US/US]; 1750 Smoke Ridge Drive, Colorado Springs, CO 80918 (US). CHEN, Bing [US/US]; 6040 Breeze Court, Colorado Springs, CO 80919 (US). VANDERSLUIS, Kristan [US/US]; 4385 Granby Circle, Colorado Springs, CO 80918 (US).

(72) Inventor: JUN, Fang (deceased).

(74) Agents: WARREN, Sanford, E., Jr.; Warren & Perez, Suite 710, 8411 Preston Road, Dallas, TX 75225 (US) et al.

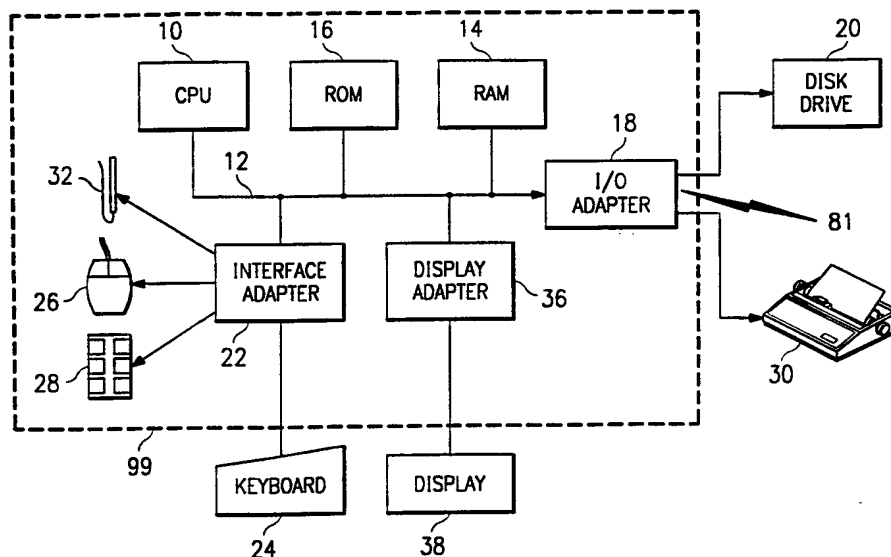
(81) Designated States: AU, CA, GM, GW, ID, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published*With international search report.**Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(88) Date of publication of the international search report:

23 December 1998 (23.12.98)

(54) Title: A COMMUNICATION SYSTEM ARCHITECTURE



(57) Abstract

A system and method for routing telephone calls, data and other multimedia information through a hybrid network which may include transfer of information across the internet. Profile information is utilized by the system throughout the media experience for routing, billing, monitoring, reporting and other media control functions. The system can include prioritized routing. The system can also facilitate callback sessions and present a display to a caller via a web page that includes status information pertaining to the callback session. Calls and callbacks can also be routed over the hybrid network. Through use of the system, users can manage more aspects of a network than previously possible, and may control network activities from a central site.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

- 1 -

A COMMUNICATION SYSTEM ARCHITECTURE

Field Of The Invention

The present invention relates to the marriage of the Internet with telephony systems, and more specifically, to a system, method and article of manufacture for using the Internet as the communication backbone of a communication system architecture while maintaining a rich array of call processing features.

10 The present invention relates to the interconnection of a communication network including telephony capability with the Internet. The Internet has increasingly become the communication network of choice for the user marketplace. Recently, software companies have begun to investigate the transfer of telephone calls across the Internet. However, the system features
15 that users demand of normal call processing are considered essential for call processing on the Internet. Today, those features are not available on the Internet.

Background of the Invention

20 In relation to the callback features of the invention, a short background will now be described.

The Internet has increasingly become the communication network of choice for the consumer e-mail marketplace. Recently, software companies have
25 begun to investigate the transfer of telephone calls across the Internet. However, the system features that users demand of normal call processing are considered essential for call processing the Internet. Today, those features are not available on the Internet. Thus, a system is required that connects the communication network including telephony capability with
30 the Internet to facilitate callback processing.

-2-

Callback scenarios for reserving calls over existing telephony networks have been available for some time. Examples of such service are CSI Callback, Rumilla Telecommunication for international callback and SummitLink which provides international callback offering distribution, wholesaling and rebilling features. The Internet provides a website entitled, ACallback on the Net@ which purports to Acollect all available information on callback services.@ This information was accumulated by doing a Yahoo search utilizing the search term Acallback@.

- 10 International callback as provided by the prior art system refers to a user being able to dial a number to connect to a switch overseas. The caller allows the phone to ring twice and hangs up. The switch then utilizes the ANI and/or called number information to query a database of profile information stored on the switch to determine billing and other information on the caller. Then, the switch initiates a call to the caller and when the caller goes offhook, the switch provides a dialtone allowing the caller to access any number available to the switch. In this way, international or other long distance callers can obtain low cost long distance services so long as they are pre-registered for the service. This service still requires the caller to be responsible for all of the overhead associated with initiating call processing, requires a caller to learn the protocol of interfacing with the switch, does not provide reservation of such services such as conferencing and it does not allow operator assistance on the calls.
- 25 Recently, AT&T has announces a service very similar to conferenceMCI (MCI=s Operator Call-in Conference Call capability). This service termed AOn-Line TeleConference@ capability allows teleconference customers to use an on-line interface to allow customers to pre-arrange an AT&T TeleConference call through the World Wide Web. However, while conference call definition of a number for each participate to call into to join the conference is provided Aall voice connections are established over the existing telephone network@ and require all parties to contact a common

-3-

number to establish the conference call (AT&T TeleConference Service: On-Line Trial Information, 2/7/97).

While this new AT&T service is moving in the direction that the subject
5 invention has already arrived at, it does not provide integration of voice over
the Internet with existing network services, nor does it provide any mention
of a callback architecture which allows a calling party to pre-arrange for a
network service to contact one or more parties and effectively eliminate the
need for any manual intervention. Moreover, it does not provide an operator
10 on an exception basis for Internet telephony operations. Thus, a true union
of the Internet and existing telephony networks is not provided.

What is needed is a method, system and article of manufacture for
facilitating callback service, providing operation assist on Internet telephony
15 operations, allowing a caller to reserve a time for a call, facilitating Internet
telephony operations to be added to a callback service, adding a
multidimensional conferencing feature to existing telephony networking and
providing an expert system to provide self-regulation of a call system.
Further, the method and system is required which is reliable, responsive
20 and effective in interfacing with existing telecommunication networks.

SUMMARY OF THE INVENTION

According to a broad aspect of a preferred embodiment of the invention,
telephone calls, data and other multimedia information is routed through a
25 switched network which includes transfer of information across the Internet
which may utilize telephony routing information and Internet protocol
address information. A telephony order entry procedure captures complete
user profile information for a user. This profile information is used by the
system throughout the telephony experience for routing, billing, monitoring,
30 reporting and other telephony control functions. Users can manage more
aspects of a network than previously possible and control network activities
from a central site, while still allowing the operator of the telephone system

-4-

to maintain quality and routing selection.

In another aspect of a preferred embodiment of the invention, a hybrid telecommunications system includes a switched communications network.

5 A packet transmission network is coupled to the switched communications network. A call router is coupled to the switched communications network and the packet transmission network. A memory is coupled to the call router and having stored therein a call parameter database. The call router is configured to route a telephone call over the switched communications
10 network and the packet transmission network based on at least one call parameter from the call parameter database. The call router is further configured to provide an intelligent service platform. The intelligent service platform includes an automated response unit with a plurality of functions available from a single connection.

15

In a further aspect of a preferred embodiment of the invention, a method for directing calls in a hybrid telecommunications system including a switched communications network and a packet transmission network stores a call parameter database in a memory. A call is received on the system. The call
20 parameter database is accessed to determine at least one call parameter. The call is routed over the switched communications network and the packet transmission network based on the at least one call parameter. An automated response unit is provided. A plurality of functions is made available from a single connection to the automated response unit.

25

In still another aspect of a preferred embodiment of the invention, a computer program embodied on a computer-readable medium for directing calls in a hybrid telecommunications system including a switched communications network and a packet transmission network has first
30 software that stores a call parameter database in a memory. Second software accesses the call parameter database when the system receives a call to determine at least one call parameter. Third software routes the call

-5-

over the switched communications network and the packet transmission network based on the at least one call parameter. Fourth software provides an automated response unit. Fifth software makes a plurality of functions available from a single connection to the automated response unit.

5

In another aspect of a preferred embodiment of the invention, telephone calls, data and other multimedia information is routed through a switched network which includes transfer of information across the Internet to provide multi-routed and multidimensional callback processing. A telephony order entry procedure captures complete user profile information for a callback operation. This profile information is used by the system throughout the telephony experience for routing, billing, monitoring, reporting and other telephony control functions. Users can manage more aspects of telephony experience and as necessary can specify a date and time for a callback telephony experience to occur. Operator assistance may also be included in the system. A display may also be included in the system. The display may include status information. The display can be provided via a web page. The status information can include information pertaining to a callback session.

20

DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages are better understood from the following detailed description of a preferred embodiment of the invention, with reference to the drawings, in which:

25

Figure **1A** is a block diagram of a representative hardware environment in accordance with a preferred embodiment;

30

Figure **1B** is a block diagram illustrating the architecture of a typical Common Channel Signaling System #7 (SS7) network in accordance with a preferred embodiment;

-6-

Figure **1C** is a block diagram of an internet telephony system in accordance with a preferred embodiment;

5 Figure **1D** is a block diagram of a hybrid switch in accordance with a preferred embodiment;

Figure **1E** is a block diagram of the connection of a hybrid switch in accordance with a preferred embodiment;

10

Figure **1F** is a block diagram of a hybrid (internet-telephony) switch in accordance with a preferred embodiment;

15 Figure **1G** is a block diagram showing the software processes involved in the hybrid internet telephony switch in accordance with a preferred embodiment;

Figure **2** is a block diagram illustrating the use of PMUs in a typical SS7 network in accordance with a preferred embodiment;

20

Figure **3** is a block diagram illustrating the systems architecture of the preferred embodiment;

25 Figure **4** is a high-level process flowchart illustrating the logical system components in accordance with a preferred embodiment;

Figures **5 - 9** are process flowcharts illustrating the detailed operation of the components illustrated in Figure **4** in accordance with a preferred embodiment;

30

Figure **10A** illustrates a Public Switched Telephone Network (PSTN) **1000** comprising a Local Exchange Carrier (LEC) **1020** through which a calling

-7-

party uses a telephone **1021** or computer **1030** to gain access to a switched network in accordance with a preferred embodiment;

Figure **10B** illustrates an internet routing network in accordance with a preferred embodiment;

Figure **11** illustrates a VNET Personal Computer (PC) to PC Information call flow in accordance with a preferred embodiment;

Figure **12** illustrates a VNET Personal Computer (PC) to out-of-network PC Information call flow in accordance with a preferred embodiment;

Figure **13** illustrates a VNET Personal Computer (PC) to out-of-network Phone Information call flow in accordance with a preferred embodiment;

Figure **14** illustrates a VNET Personal Computer (PC) to in-network Phone Information call flow in accordance with a preferred embodiment;

Figure **15** illustrates a personal computer to personal computer internet telephony call in accordance with a preferred embodiment;

Figure **16** illustrates a phone call that is routed from a PC through the Internet to a phone in accordance with a preferred embodiment;

Figure **17** illustrates a phone to PC call in accordance with a preferred embodiment;

Figure **18** illustrates a phone to phone call over the internet in accordance with a preferred embodiment;

Figure **19A** and **19B** illustrate an Intelligent Network in accordance with a preferred embodiment;

Figure **19C** illustrates a Video-Conferencing Architecture in accordance with a preferred embodiment;

- 5 Figure **19D** illustrates a Video Store and Forward Architecture in accordance with a preferred embodiment;

Figure **19E** illustrates an architecture for transmitting video telephony over the Internet in accordance with a preferred embodiment;

10

Figure **19F** is a block diagram of an internet telephony system in accordance with a preferred embodiment;

- 15 Figure **19G** is a block diagram of a prioritizing access/router in accordance with a preferred embodiment;

Figure **20** is a high level block diagram of a networking system in accordance with a preferred embodiment;

- 20 Figure **21** is a functional block diagram of a portion of the system shown in Figure **20** in accordance with a preferred embodiment;

Figure **22** is another high level block diagram in accordance with a preferred embodiment of Figure **21**;

25

Figure **23** is a block diagram of a switchless network system in accordance with a preferred embodiment;

- 30 Figure **24** is a hierarchy diagram illustrating a portion of the systems shown in Figures **20** and **23** in accordance with a preferred embodiment;

Figure **25** is a block diagram illustrating part of the system portion shown in

-9-

Figure **24** in accordance with a preferred embodiment;

Figure **26** is a flow chart illustrating a portion of a method in accordance with a preferred embodiment;

5

Figures **27-39** are block diagrams illustrating further aspects of the systems of Figures **20** and **23** in accordance with a preferred embodiment;

Figure **40** is a diagrammatic representation of a web server logon in accordance with a preferred embodiment;

10

Figure **41** is a diagrammatic representation of a server directory structure used with the logon of Figure **40** in accordance with a preferred embodiment;

15

Figure **42** is a more detailed diagrammatic representation of the logon of Figure **40** in accordance with a preferred embodiment;

20

Figures **43-50** are block diagrams illustrating portions of the hybrid network in accordance with a preferred embodiment;

Figure **51** illustrates a configuration of the Data Management Zone (DMZ) **5105** in accordance with a preferred embodiment;

25

Figures **52A-52C** illustrate network block diagrams in connection with a dial-in environment in accordance with a preferred embodiment;

Figure **53** depicts a flow diagram illustrating the fax tone detection in accordance with a preferred embodiment;

30

Figures **54A** through **54E** depict a flow diagram illustrating the VFP Completion process for fax and voice mailboxes in accordance with a

-10-

preferred embodiment;

Figures **55A** and **55B** illustrate the operation of the Pager Termination processor in accordance with a preferred embodiment;

5

Figure **56** depicts the GetCallback routine called from the pager termination in accordance with a preferred embodiment;

Figure **57** shows a user login screen for access to online profile management in accordance with a preferred embodiment;

10

Figure **58** shows a call routing screen, used to set or change a user's call routing instructions in accordance with a preferred embodiment;

Figure **59** shows a guest menu configuration screen, used to set up a guest menu for presentation to a caller who is not an account owner in accordance with a preferred embodiment;

15

Figure **60** shows an override routing screen, which allows a user to route all calls to a selected destination in accordance with a preferred embodiment;

20

Figure **61** shows a speed dial numbers screen, used to set up speed dial in accordance with a preferred embodiment;

Figure **62** shows a voicemail screen, used to set up voicemail in accordance with a preferred embodiment;

25

Figure **63** shows a faxmail screen, used to set up faxmail in accordance with a preferred embodiment;

30

Figure **64** shows a call screening screen, used to set up call screening in accordance with a preferred embodiment;

- 11 -

Figures **65-67** show supplemental screens used with user profile management in accordance with a preferred embodiment;

- 5 Figure **68** is a flow chart showing how the validation for user entered speed dial numbers is carried out in accordance with a preferred embodiment;

- Figures **69A-69AI** are automated response unit (ARU) call flow charts showing software implementation in accordance with a preferred
10 embodiment;

Figures **70A-70R** are console call flow charts further showing software implementation in accordance with a preferred embodiment;

- 15 Figure **71** illustrates a typical customer configuration for a VNET to VNET system in accordance with a preferred embodiment;

- Figure **72** illustrates the operation of DAPs in accordance with a preferred
20 embodiment;

Figure **73** illustrates the process by which a telephone connects to a release link trunk for 1-800 call processing in accordance with a preferred
embodiment;

- 25 Figure **74** illustrates the customer side of a DAP procedure request in accordance with a preferred embodiment;

Figure **75** illustrates operation of the switch **10530** to select a particular number or "hotline" for a caller in accordance with a preferred embodiment;

- 30 Figure **76** illustrates the operation of a computer-based voice gateway for selectively routing telephone calls through the Internet in accordance with a

-12-

preferred embodiment;

Figure **77** illustrates the operation of the VRU of figure **76** deployed in a centralized architecture in accordance with a preferred embodiment;

5

Figure **78** illustrates the operation of the VRU of figure **76** deployed in a distributed architecture in accordance with a preferred embodiment;

Figure **79A** and **79B** illustrate the operation of sample applications for Internet call routing in accordance with a preferred embodiment;

10

Figure **79B** illustrates a number of applications for caller-initiated consumer transactions in accordance with a preferred embodiment;

Figure **80** illustrates a configuration of a switching network offering voice mail and voice response unit services, as well as interconnection into a service provider, in accordance with a preferred embodiment;

15

Figure **81** illustrates an inbound shared Automated Call Distributor (ACD) call with data sharing through a database in accordance with a preferred embodiment;

20

Figure **82** is a block diagram of an exemplary telecommunications system in accordance with a preferred embodiment;

25

Figure **83** is a block diagram of an exemplary computer system in accordance with a preferred embodiment;

Figure **84** illustrates the CDR and PNR call record formats in accordance with a preferred embodiment;

30

Figures **85(A)** and **85(B)** collectively illustrate the ECDR and EPNR call

-13-

record formats in accordance with a preferred embodiment;

Figure **86** illustrates the OSR and POSR call record formats in accordance with a preferred embodiment;

5

Figures **87(A)** and **87(B)** collectively illustrate the EOSR and EPOSr call record formats in accordance with a preferred embodiment;

Figure **88** illustrates the SER call record format in accordance with a preferred embodiment;

10

Figures **89(A)** and **89(B)** are control flow diagrams illustrating the conditions under which a switch uses the expanded record format in accordance with a preferred embodiment;

15

Figure **90** is a control flow diagram illustrating the Change Time command in accordance with a preferred embodiment;

Figure **91** is a control flow diagram illustrating the Change Daylight Savings Time command in accordance with a preferred embodiment;

20

Figure **92** is a control flow diagram illustrating the Network Call Identifier (NCID) switch call processing in accordance with a preferred embodiment;

Figure **93** is a control flow diagram illustrating the processing of a received Network Call Identifier in accordance with a preferred embodiment;

25

Figure **94(A)** is a control flow diagram illustrating the generation of a Network Call Identifier in accordance with a preferred embodiment;

30

Figure **94(B)** is a control flow diagram illustrating the addition of a Network Call Identifier to a call record in accordance with a preferred embodiment;

Figure **95** is a control flow diagram illustrating the transport of a call in accordance with a preferred embodiment;

- 5 Figure **96** shows a hardware component embodiment for allowing a video operator to participate in a video conferencing platform, providing services including but not limited to monitoring, viewing and recording any video conference call and assisting the video conference callers in accordance with a preferred embodiment;

10

Figure **97** shows a system for enabling a video operator to manage video conference calls which includes a video operator console system in accordance with a preferred embodiment;

- 15 Figure **98** shows a system for enabling a video operator to manage video conference calls which includes a video operator console system in accordance with a preferred embodiment;

20 Figure **99** shows how a video conference call initiated by the video operator in accordance with a preferred embodiment;

Figure **100** shows the class hierarchy for video operator software system classes in accordance with a preferred embodiment;

- 25 Figure **101** shows a state transition diagram illustrating the state changes that may occur in the VOCall object's m_state variable in accordance with a preferred embodiment;

30 Figure **102** shows a state transition diagram illustrating the state changes that may occur in the VOConnection object's m_state variable ("state variable") in accordance with a preferred embodiment;

-15-

Figure **103** shows a state transition diagram illustrating the state changes that may occur in the VOConference object's m_state variable ("state variable") in accordance with a preferred embodiment;

- 5 Figure **104** shows a state transition diagram illustrating the state changes that may occur in the VORecorder object's m_state variable ("state variable") in accordance with a preferred embodiment;

- 10 Figure **105** shows a state transition diagram illustrating the state changes that may occur in the VORecorder object's m_state variable ("state variable") in accordance with a preferred embodiment;

- 15 Figure **106** shows the class hierarchy for the video operator graphics user interface ("GUI") classes in accordance with a preferred embodiment;

Figure **107** shows a database schema for the video operator shared database in accordance with a preferred embodiment;

- 20 Figure **108** shows one embodiment of the Main Console window in accordance with a preferred embodiment;

Figure **109** shows one embodiment of the Schedule window in accordance with a preferred embodiment;

- 25 Figure **110** shows one embodiment of the Conference window **41203**, which is displayed when the operator selects a conference or playback session in the Schedule window in accordance with a preferred embodiment;

- 30 Figure **111** shows one embodiment of the Video Watch window **41204**, which displays the H.320 input from a selected call of a conference connection or a separate incoming or outgoing call in accordance with a preferred embodiment;

-16-

Figure **112** shows one embodiment of the Console Output window **41205** which displays all error messages and alerts in accordance with a preferred embodiment; and

5

Figure **113** shows a Properties dialog box in accordance with a preferred embodiment.

Figure **114A** is a block diagram of an access/router system in accordance with a preferred embodiment.

10

Figure **114B** is a block diagram of the architecture in accordance with a preferred embodiment.

15

Figure **115** is a block diagram of an internet based callback architecture in accordance with a preferred embodiment.

DETAILED DESCRIPTION**TABLE OF CONTENTS**

	I. THE COMPOSITION OF THE INTERNET	28
	II. PROTOCOL STANDARDS	29
5	A. Internet Protocols	29
	B. International Telecommunication Union-Telecommunication Standardization Sector ("ITU-T") Standards	29
	III. TCP/IP FEATURES.....	32
	IV. INFORMATION TRANSPORT IN COMMUNICATION NETWORKS	32
10	A. Switching Techniques.....	32
	B. Gateways and Routers	36
	C. Using Network Level Communication for Smooth User Connection	38
	D. Datagrams and Routing	39
15	V. TECHNOLOGY INTRODUCTION	40
	A. ATM	40
	B. Frame Relay	41
	C. ISDN	41
	VI. MCI INTELLIGENT NETWORK.....	41
20	A. Components of the MCI Intelligent Network.....	43
	1. MCI Switching Network.....	43
	2. Network Control System/Data Access Point (NCS/DAP)	44
	3. Intelligent Services Network (ISN) 4	44
	4. Enhanced Voice Services (EVS) 9.....	45
25	5. Additional Components.....	45

	B. Intelligent Network System Overview	47
	C. Call Flow Example	48
	VII. ISP FRAMEWORK	50
	A. Background	50
5	1. Broadband Access	50
	2. Internet Telephony System	51
	3. Capacity	56
	4. Future Services	57
	B. ISP Architecture Framework	58
10	C. ISP Functional Framework	59
	D. ISP Integrated Network Services	62
	E. ISP Components	63
	F. Switchless Communications Services	63
	G. Governing Principles	64
15	1. Architectural Principles	64
	2. Service Feature Principles	65
	3. Capability Principles	66
	4. Service Creation, Deployment, and Execution Principles	67
	5. Resource Management Model 2150 Principles	67
20	6. Data Management 2138 Principles	69
	7. Operational Support Principles	71
	8. Physical Model Principles	72
	H. ISP Service Model	73
	1. Purpose	73
25	2. Scope of Effort	74
	3. Service Model Overview	75
	4. Service Structure	75
	5. Service 2200 Execution	79
	6. Service Interactions	80
30	7. Service Monitoring	81

	I. ISP Data Management Model	82
	1. Scope	82
	2. Purpose	82
	3. Data management Overview	83
5	4. Logical Description	86
	5. Physical Description	91
	6. Technology Selection	92
	7. Implementations	93
	8. Security	93
10	9. Meta-Data	94
	10. Standard Database Technologies	94
	J. ISP Resource Management Model	94
	2. The Local Resource Manager (LRM):	99
	3. The Global Resource Manager (GRM) 2188:	99
15	4. The Resource Management Model (RMM)	99
	5. Component Interactions	102
	K. Operational Support Model	105
	1. Introduction	105
	2. The Operational Support Model	107
20	3. The Protocol Model	112
	4. The Physical Model	113
	5. Interface Points	113
	6. General	114
	L. Physical Network Model	116
25	1. Introduction	116
	2. Information Flow	116
	3. Terminology	118
	4. Entity Relationships	119
	VIII. INTELLIGENT NETWORK	120
30	A. Network Management	120

	B. Customer Service	121
	C. Accounting.....	122
	D. Commissions	123
	E. Reporting	123
5	F. Security	123
	G. Trouble Handling	123
	IX. ENHANCED PERSONAL SERVICES	124
	A. Web Server Architecture	124
	1. Welcome Server 450	124
10	2. Token Server 454	125
	3. Application Servers	127
	B. Web Server System Environment.....	129
	1. Welcome Servers	129
	2. Token Servers 454	132
15	3. Profile Management Application Servers	133
	C. Security	133
	D. Login Process.....	135
	E. Service Selection	136
	F. Service Operation	136
20	1. NIDS Server	137
	2. TOKEN database service.....	138
	3. SERVERS database service.	139
	4. HOSTILE_IP database service.	139
	5. TOKEN_HOSTS database service.	140
25	6. SERVER_ENV database service.	141
	7. Chron Job(s)	141
	G. Standards	142
	H. System Administration.....	142
	I. Product/Enhancement	143
30	J. Interface Feature Requirements (Overview)	144

	1. The User Account Profile	145
	2. The Database of Messages	146
	K. Automated Response Unit (ARU) Capabilities	146
	1. User Interface	146
5	L. Message Management	149
	1. Multiple Media Message Notification	149
	2. Multiple Media Message Manipulation	150
	3. Text to Speech	150
	4. Email Forwarding to a Fax Machine	151
10	5. Pager Notification of Messages Received	151
	6. Delivery Confirmation of Voicemail	151
	7. Message Prioritization	152
	M. Information Services	152
	N. Message Storage Requirements	153
15	O. Profile Management	153
	P. Call Routing Menu Change	154
	Q. Two-way Pager Configuration Control and Response to Park and Page	155
	R. Personalized Greetings	155
20	S. List Management	155
	T. Global Message Handling	156
	X. INTERNET TELEPHONY AND RELATED SERVICES	157
	A. System Environment for Internet Media	159
	1. Hardware	159
25	2. Object-Oriented Software Tools	159
	B. Telephony Over The Internet	167
	1. Introduction	168
	2. IP Phone as a Commercial Service	171
	3. Phone Numbers in the Internet	180
30	4. Other Internet Telephony Carriers	181

-22-

	5. International Access	181
	C. Internet Telephony Services	188
	D. Call Processing	194
	1. VNET Call Processing	195
5	2. Descriptions of Block Elements	198
	E. Re-usable Call Flow Blocks	203
	1. VNET PC connects to a corporate intranet and logs in to a directory service	203
10	2. VNET PC queries a directory service for a VNET translation	207
	3. PC connects to an ITG	209
	4. ITG connects to a PC	210
	5. VNET PC to PC Call Flow Description	211
15	6. Determining best choice for Internet client selection of an Internet Telephony Gateway server on the Internet:	212
	7. Vnet Call Processing	220
	XI. TELECOMMUNICATION NETWORK MANAGEMENT	227
	A. SNMS Circuits Map	246
20	B. SNMS Connections Map	246
	C. SNMS Nonadjacent Node Map	247
	D. SNMS LATA Connections Map	247
	E. NPA-NXX Information List	247
	F. End Office Information List	247
25	G. Trunk Group Information List	248
	H. Filter Definition Window	248
	I. Trouble Ticket Window	248
	XII. VIDEO TELEPHONY OVER POTS	249
	A. Components of Video Telephony System	250

	1. DSP modem pools with ACD.....	250
	2. Agent	251
	3. Video on Hold Server.....	251
	4. Video Mail Server	251
5	5. Video Content Engine.....	251
	6. Reservation Engine	252
	7. Video Bridge	252
	B. Scenario.....	252
	C. Connection Setup	252
10	D. Calling the Destination	254
	E. Recording Video-Mail, Store & Forward Video and Greetings	254
	F. Retrieving Video-Mail and Video On Demand.....	255
	G. Video-conference Scheduling	255
	XIII. VIDEO TELEPHONY OVER THE INTERNET	256
15	A. Components.....	257
	1. Directory and Registry Engine	258
	2. Agents	258
	3. Video Mail Server	258
	4. Video Content Engine.....	258
20	5. Conference Reservation Engine	258
	6. MCI Conference Space	259
	7. Virtual Reality Space Engine	259
	B. Scenario.....	259
	C. Connection Setup	259
25	D. Recording Video-Mail, Store & Forward Video and Greetings	260
	E. Retrieving Video-Mail and Video On Demand.....	261
	F. Video-conference Scheduling.....	261
	G. Virtual Reality.....	261
	XIV. VIDEO-CONFERENCING ARCHITECTURE	262

	A. Features.....	262
	B. Components.....	263
	1. End-User Terminals	263
	2. LAN Interconnect System	263
5	3. ITU H.323 Server.....	264
	4. Gatekeeper.....	264
	5. Operator Services Module	265
	6. Multipoint Control Unit (MCU)	265
	7. Gateway.....	266
10	8. Support Service Units	266
	C. Overview	266
	D. Call Flow Example	268
	1. Point-to-Point Calls	268
	2. Multipoint Video-Conference Calls	272
15	E. Conclusion.....	273
	XV. VIDEO STORE AND FORWARD ARCHITECTURE	273
	A. Features.....	274
	B. Architecture	274
	C. Components.....	274
20	1. Content Creation and Transcoding.....	274
	2. Content Management and Delivery	275
	3. Content Retrieval and Display	275
	D. Overview	276
	XVI. VIDEO OPERATOR	278
25	A. Hardware Architecture	278
	B. Video Operator Console.....	281
	C. Video Conference Call Flow	286
	D. Video Operator Software System	287
	1. Class Hierarchy	287

	2. Class and Object details	289
	E. Graphical User Interface Classes	333
	1. Class Hierarchy	333
	2. Class and Object details	336
5	F. Video Operator Shared Database	355
	1. Database Schema	355
	G. Video Operator Console Graphical User Interface Windows	357
	1. Main Console Window	357
	2. Schedule Window	357
10	3. Conference Window	357
	4. Video Watch Window	360
	5. Console Output Window	361
	6. Properties Dialog Box	361
	XVII. WORLD WIDE WEB (WWW) BROWSER CAPABILITIES	361
15	A. User Interface	361
	B. Performance	362
	C. Personal Home Page	364
	1. Storage Requirements	365
	2. On Screen Help Text	366
20	3. Personal Home Page Directory	366
	4. Control Bar	367
	5. Home Page	367
	6. Security Requirements	367
	7. On Screen Help Text	368
25	8. Profile Management	369
	9. Information Services Profile Management	371
	10. Personal Home Page Profile Management	373
	11. List Management	374
	12. Global Message Handling	376
30	D. Message Center	376

	1. Storage Requirements	379
	E. PC Client Capabilities	380
	1. User Interface	380
	2. Security	381
5	3. Message Retrieval	381
	4. Message Manipulation	383
	F. Order Entry Requirements	383
	1. Provisioning and Fulfillment	387
	G. Traffic Systems	387
10	H. Pricing	387
	I. Billing	388
	 XVIII. DIRECTLINE MCI	388
	A. Overview	389
	1. The ARU (Audio Response Unit) 502	389
15	2. The VFP (Voice Fax Platform) 504	389
	3. The DDS (Data Distribution Service) 506	389
	B. Rationale	390
	C. Detail	390
	1. Call Flow Architecture 520	391
20	2. Network Connectivity	391
	3. Call Flow	392
	4. Data Flow Architecture	394
	D. Voice Fax Platform (VFP) 504 Detailed Architecture	395
	1. Overview	395
25	2. Rationale	395
	3. Detail	397
	E. Voice Distribution Detailed Architecture	401
	1. Overview	401
	2. Rationale	401
30	F. Login Screen	421

-27-

	G. Call Routing Screen	422
	H. Guest Menu Configuration Screen	424
	I. Override Routing Screen	426
	J. Speed Dial Screen	427
5	K. ARU CALL FLOWS	437
	 XIX. INTERNET FAX	 530
	A. Introduction	530
	B. Details	531
	 XX. INTERNET SWITCH TECHNOLOGY	 534
10	A. An Embodiment	534
	B. Another Embodiment	545
	 XXI. BILLING	 549
	A. An Embodiment	553
	1. Call Record Format	553
15	2. Network Call Identifier	554
	B. [Another Embodiment]	556
	1. Call Record Format	556
	2. Network Call Identifier	565

-28-

INTRODUCTION TO THE INTERNET**I. THE COMPOSITION OF THE INTERNET**

The Internet is a method of interconnecting physical networks and a set of conventions for using networks that allow the computers they reach to interact. Physically, the Internet is a huge, global network spanning over 92 countries and comprising 59,000 academic, commercial, government, and military networks, according to the Government Accounting Office (GAO), with these numbers expected to double each year. Furthermore, there are about 10 million host computers, 50 million users, and 76,000 World-Wide Web servers connected to the Internet. The backbone of the Internet consists of a series of high-speed communication links between major supercomputer sites and educational and research institutions within the U.S. and throughout the world.

Before progressing further, a common misunderstanding regarding the usage of the term "internet" should be resolved. Originally, the term was used only as the name of the network based upon the Internet Protocol, but now, internet is a generic term used to refer to an entire class of networks. An "internet" (lowercase "i") is any collection of separate physical networks, interconnected by a common protocol, to form a single logical network, whereas the "Internet" (uppercase "I") is the worldwide collection of interconnected networks that uses Internet Protocol to link the large number of physical networks into a single logical network.

II. PROTOCOL STANDARDS

A. *Internet Protocols*

5 Protocols govern the behavior along the Internet backbone and thus set
down the key rules for data communication. Transmission Control
Protocol/Internet Protocol (TCP/IP) has an open nature and is available to
everyone, meaning that it attempts to create a network protocol system that
10 is independent of computer or network operating system and architectural
differences. As such, TCP/IP protocols are publicly available in standards
documents, particularly in Requests for Comments (RFCs). A requirement
for Internet connection is TCP/IP, which consists of a large set of data
communications protocols, two of which are the Transmission Control
Protocol and the Internet Protocol. An excellent description of the details
15 associated with TCP/IP and UDP/IP is provided in TCP/IP Illustrated, W.
Richard Stevens, Addison-Wesley Publishing Company (1996).

B. *International Telecommunication Union- Telecommunication Standardization Sector ("ITU-T") Standards*

20

The International Telecommunication Union-Telecommunication
Standardization Sector ("ITU-T") has established numerous standards
governing protocols and line encoding for telecommunication devices.

25 Because many of these standards are referenced throughout this document,
summaries of the relevant standards are listed below for reference.

ITU G.711 Recommendation for Pulse Code Modulation of 3kHz Audio
Channels.

ITU G.722 Recommendation for 7kHz Audio Coding within a 64kbit/s channel.

ITU G.723 Recommendation for dual rate speech coder for multimedia communication transmitting at 5.3 and 6.3 kbits.

- 5 **ITU G.728** Recommendation for coding of speech at 16kbit/s using low-delay code excited linear prediction (LD-CELP)

ITU H.221 Frame Structure for a 64 to 1920 kbit/s Channel in Audiovisual Teleservices

ITU H.223 Multiplexing Protocols for Low Bitrate Multimedia Terminals

- 10 **ITU H.225** ITU Recommendation for Media Stream Packetization and Synchronization on non-guaranteed quality of service LANs.

ITU H.230 Frame-synchronous Control and Indication Signals for Audiovisual Systems

- 15 **ITU H.231** Multipoint Control Unit for Audiovisual Systems Using Digital Channels up to 2 Mbit/s

ITU H.242 System for Establishing Communication Between Audiovisual Terminals Using Digital Channels up to 2Mbits

ITU H.243 System for Establishing Communication Between Three or More Audiovisual Terminals Using Digital Channels up to 2 Mbit/s

- 20 **ITU H.245** Recommendation for a control protocol for multimedia communication

ITU H.261 Recommendation for Video Coder-Decoder for audiovisual services supporting video resolutions of 352x288 pixels and 176x144 pixels.

- 25 **ITU H.263** Recommendation for Video Coder-Decoder for audiovisual services supporting video resolutions of 128x96 pixels, 176x144 pixels, 352x288 pixels, 704x576 pixels and 1408x1152 pixels.

ITU H.320 Recommendation for Narrow Band ISDN visual telephone systems.

ITU H.321 Visual Telephone Terminals over ATM

- 30 **ITU H.322** Visual Telephone Terminals over Guaranteed Quality of Service LANs

ITU H.323 ITU Recommendation for Visual Telephone Systems and

-31-

Equipment for Local Area Networks which provide a non-guaranteed quality of service.

ITU H.324 Recommendation for Terminals and Systems for low bitrate(28.8 Kbps) multimedia communication on dial-up telephone lines.

5 **ITU T.120** Transmission Protocols for Multimedia Data.

In addition, several other relevant standards are referenced in this document:

10 **ISDN** Integrated Services Digital Network, the digital communication standard for transmission of voice, video and data on a single communications link.

RTP Real-Time Transport Protocol, an Internet Standard Protocol for transmission of real-time data like voice and video over unicast and
15 multicast networks.

IP Internet Protocol, an Internet Standard Protocol for transmission and delivery of data packets on a packet switched network of interconnected computer systems.

PPP Point-to-Point Protocol

20 **MPEG** Motion Pictures Expert Group, a standards body under the International Standards Organization(ISO), Recommendations for compression of digital Video and Audio including the bit stream but not the compression algorithms.

SLIP Serial Line Internet Protocol

25 **RSVP** Resource Reservation Setup Protocol

UDP User Datagram Protocol

III. TCP/IP FEATURES

The popularity of the TCP/IP protocols on the Internet grew rapidly because they met an important need for worldwide data communication and had

5 several important characteristics that allowed them to meet this need.

These characteristics, still in use today, include:

A common addressing scheme that allows any device running TCP/IP to uniquely address any other device on the Internet.

10 Open protocol standards, freely available and developed independently of any hardware or operating system. Thus, TCP/IP is capable of being used with different hardware and software, even if Internet communication is not required.

15 Independence from any specific physical network hardware, allows TCP/IP to integrate many different kinds of networks. TCP/IP can be used over an Ethernet, a token ring, a dial-up line, or virtually any other kinds of physical transmission media.

IV. INFORMATION TRANSPORT IN COMMUNICATION NETWORKS

20

A. *Switching Techniques*

An understanding of how information travels in communication systems is required to appreciate the recent steps taken by key players in today's

Internet backbone business. The traditional type of communication network

25 is circuit switched. The U.S. telephone system uses such circuit switching techniques. When a person or a computer makes a telephone call, the switching equipment within the telephone system seeks out a physical path from the originating telephone to the receiver's telephone. A circuit-switched network attempts to form a dedicated connection, or circuit, between these

-33-

two points by first establishing a circuit from the originating phone through the local switching office, then across trunk lines, to a remote switching office, and finally to the destination telephone. This dedicated connection exists until the call terminates.

5

The establishment of a completed path is a prerequisite to the transmission of data for circuit switched networks. After the circuit is in place, the microphone captures analog signals, and the signals are transmitted to the Local Exchange Carrier (LEC) Central Office (CO) in analog form over an analog loop. The analog signal is not converted to digital form until it reaches the LEC Co, and even then only if the equipment is modern enough to support digital information. In an ISDN embodiment, however, the analog signals are converted to digital at the device and transmitted to the LEC as digital information.

15

Upon connection, the circuit guarantees that the samples can be delivered and reproduced by maintaining a data path of 64 Kbps (thousand bits per second). This rate is not the rate required to send digitized voice per se. Rather, 64Kbps is the rate required to send voice digitized with the Pulse Code Modulated (PCM) technique. Many other methods for digitizing voice exist, including ADPCM (32Kbps), GSM (13 Kbps), TrueSpeech 8.5 (8.5 Kbps), G.723 (6.4 Kbps or 5.3 Kbps) and Voxware RT29HQ (2.9 Kbps). Furthermore, the 64 Kbps path is maintained from LEC Central Office (CO) Switch to LEC CO, but not from end to end. The analog local loop transmits an analog signal, not 64 Kbps digitized audio. One of these analog local loops typically exists as the "last mile" of each of the telephone network circuits to attach the local telephone of the calling party.

25

This guarantee of capacity is the strength of circuit-switched networks. However, circuit switching has two significant drawbacks. First, the setup time can be considerable, because the call signal request may find the lines busy with other calls; in this event, there is no way to gain connection until

30

-34-

some other connection terminates. Second, utilization can be low while costs are high. In other words, the calling party is charged for the duration of the call and for all of the time even if no data transmission takes place (i.e. no one speaks). Utilization can be low because the time between
5 transmission of signals is unable to be used by any other calls, due to the dedication of the line. Any such unused bandwidth during the connection is wasted.

Additionally, the entire circuit switching infrastructure is built around 64
10 Kbps circuits. The infrastructure assumes the use of PCM encoding techniques for voice. However, very high quality codecs are available that can encode voice using less than one-tenth of the bandwidth of PCM. However, the circuit switched network blindly allocates 64 Kbps of bandwidth for a call, end-to-end, even if only one-tenth of the bandwidth is
15 utilized. Furthermore, each circuit generally only connects two parties. Without the assistance of conference bridging equipment, an entire circuit to a phone is occupied in connecting one party to another party. Circuit switching has no multicast or multipoint communication capabilities, except when used in combination with conference bridging equipment.

20 Other reasons for long call setup time include the different signaling networks involved in call setup and the sheer distance causing propagation delay. Analog signaling from an end station to a CO on a low bandwidth link can also delay call setup. Also, the call setup data travels great
25 distances on signaling networks that are not always transmitting data at the speed of light. When the calls are international, the variations in signaling networks grows, the equipment handling call setup is usually not as fast as modem setup and the distances are even greater, so call setup slows down even more. Further, in general, connection-oriented virtual or physical
30 circuit setup, such as circuit switching, requires more time at connection setup time than comparable connectionless techniques due to the end-to-end handshaking required between the conversing parties.

-35-

Message switching is another switching strategy that has been considered. With this form of switching, no physical path is established in advance between the sender and receiver; instead, whenever the sender has a block
5 of data to be sent, it is stored at the first switching office and retransmitted to the next switching point after error inspection. Message switching places no limit on block size, thus requiring that switching stations must have disks to buffer long blocks of data; also, a single block may tie up a line for many minutes, rendering message switching useless for interactive traffic.

10 Packet switched networks, which predominate the computer network industry, divide data into small pieces called packets that are multiplexed onto high capacity intermachine connections. A packet is a block of data with a strict upper limit on block size that carries with it sufficient
15 identification necessary for delivery to its destination. Such packets usually contain several hundred bytes of data and occupy a given transmission line for only a few tens of milliseconds. Delivery of a larger file via packet switching requires that it be broken into many small packets and sent one at a time from one machine to the other. The network hardware delivers
20 these packets to the specified destination, where the software reassembles them into a single file.

Packet switching is used by virtually all computer interconnections because of its efficiency in data transmissions. Packet switched networks use
25 bandwidth on a circuit as needed, allowing other transmissions to pass through the lines in the interim. Furthermore, throughput is increased by the fact that a router or switching office can quickly forward to the next stop any given packet, or portion of a large file, that it receives, long before the other packets of the file have arrived. In message switching, the
30 intermediate router would have to wait until the entire block was delivered before forwarding. Today, message switching is no longer used in computer networks because of the superiority of packet switching.

-36-

To better understand the Internet, a comparison to the telephone system is helpful. The public switched telephone network was designed with the goal of transmitting human voice, in a more or less recognizable form. Their
5 suitability has been improved for computer-to-computer communications but remains far from optimal. A cable running between two computers can transfer data at speeds in the hundreds of megabits, and even gigabits per second. A poor error rate at these speeds would be only one error per day. In contrast, a dial-up line, using standard telephone lines, has a maximum
10 data rate in the thousands of bits per second, and a much higher error rate. In fact, the combined bit rate times error rate performance of a local cable could be 11 orders of magnitude better than a voice-grade telephone line. New technology, however, has been improving the performance of these lines.

15

B. Gateways and Routers

The Internet is composed of a great number of individual networks, together forming a global connection of thousands of computer systems. After understanding that machines are connected to the individual networks, we
20 can investigate how the networks are connected together to form an internetwork, or an internet. At this point, internet gateways and internet routers come into play.

In terms of architecture, two given networks are connected by a computer
25 that attaches to both of them. Internet gateways and routers provide those links necessary to send packets between networks and thus make connections possible. Without these links, data communication through the Internet would not be possible, as the information either would not reach its destination or would be incomprehensible upon arrival. A gateway may be
30 thought of as an entrance to a communications network that performs code and protocol conversion between two otherwise incompatible networks. For

-37-

instance, gateways transfer electronic mail and data files between networks over the internet.

5 IP Routers are also computers that connect networks and is a newer term preferred by vendors. These routers must make decisions as to how to send the data packets it receives to its destination through the use of continually updated routing tables. By analyzing the destination network address of the packets, routers make these decisions. Importantly, a router does not generally need to decide which host or end user will receive a packet; instead, a router seeks only the destination network and thus keeps track of information sufficient to get to the appropriate network, not necessarily the appropriate end user. Therefore, routers do not need to be huge supercomputing systems and are often just machines with small main memories and little disk storage. The distinction between gateways and routers is slight, and current usage blurs the line to the extent that the two terms are often used interchangeably. In current terminology, a gateway moves data between different protocols and a router moves data between different networks. So a system that moves mail between TCP/IP and OSI is a gateway, but a traditional IP gateway (that connects different networks) is a router.

Now, it is useful to take a simplified look at routing in traditional telephone systems. The telephone system is organized as a highly redundant, multilevel hierarchy. Each telephone has two copper wires coming out of it that go directly to the telephone company's nearest end office, also called a local central office. The distance is typically less than 10 km; in the U.S. alone, there are approximately 20,000 end offices. The concatenation of the area code and the first three digits of the telephone number uniquely specify an end office and help dictate the rate and billing structure.

The two-wire connections between each subscriber's telephone and the end office are called local loops. If a subscriber attached to a given end office

-38-

calls another subscriber attached to the same end office, the switching mechanism within the office sets up a direct electrical connection between the two local loops. This connection remains intact for the duration of the call, due to the circuit switching techniques discussed earlier.

5

If the subscriber attached to a given end office calls a user attached to a different end office, more work has to be done in the routing of the call.

First, each end office has a number of outgoing lines to one or more nearby switching centers, called toll offices. These lines are called toll connecting
10 trunks. If both the caller's and the receiver's end offices happen to have a toll connecting trunk to the same toll office, the connection may be established within the toll office. If the caller and the recipient of the call do not share a toll office, then the path will have to be established somewhere higher up in the hierarchy. There are sectional and regional offices that
15 form a network by which the toll offices are connected. The toll, sectional, and regional exchanges communicate with each other via high bandwidth inter-toll trunks. The number of different kinds of switching centers and their specific topology varies from country to country, depending on its telephone density.

20

C. Using Network Level Communication for Smooth User Connection

In addition to the data transfer functionality of the Internet, TCP/IP also seeks to convince users that the Internet is a solitary, virtual network.

25 TCP/IP accomplishes this by providing a universal interconnection among machines, independent of the specific networks to which hosts and end users attach. Besides router interconnection of physical networks, software is required on each host to allow application programs to use the Internet as if it were a single, real physical network.

30

D. Datagrams and Routing

The basis of Internet service is an underlying, connectionless packet delivery system run by routers, with the basic unit of transfer being the packet. In internets running TCP/IP, such as the Internet backbone, these packets are
5 called datagrams. This section will briefly discuss how these datagrams are routed through the Internet.

In packet switching systems, routing is the process of choosing a path over which to send packets. As mentioned before, routers are the computers that
10 make such choices. For the routing of information from one host within a network to another host on the same network, the datagrams that are sent do not actually reach the Internet backbone. This is an example of internal routing, which is completely self-contained within the network. The machines outside of the network do not participate in these internal routing
15 decisions.

At this stage, a distinction should be made between direct delivery and indirect delivery. Direct delivery is the transmission of a datagram from one machine across a single physical network to another machine on the same
20 physical network. Such deliveries do not involve routers. Instead, the sender encapsulates the datagram in a physical frame, addresses it, and then sends the frame directly to the destination machine.

Indirect delivery is necessary when more than one physical network is
25 involved, in particular when a machine on one network wishes to communicate with a machine on another network. This type of communication is what we think of when we speak of routing information across the Internet backbone. In indirect delivery, routers are required. To send a datagram, the sender must identify a router to which the datagram
30 can be sent, and the router then forwards the datagram towards the destination network. Recall that routers generally do not keep track of the

-40-

individual host addresses (of which there are millions), but rather just keeps track of physical networks (of which there are thousands). Essentially, routers in the Internet form a cooperative, interconnected structure, and datagrams pass from router to router across the backbone until they reach a
5 router that can deliver the datagram directly.

V. TECHNOLOGY INTRODUCTION

The changing face of the internet world causes a steady inflow of new systems and technology. The following three developments, each likely to
10 become more prevalent in the near future, serve as an introduction to the technological arena:

A. ATM

Asynchronous Transfer Mode (ATM) is a networking technology using a high-
15 speed, connection-oriented system for both local area and wide area networks. ATM networks require modern hardware including:

- High speed switches that can operate at gigabit (trillion bit) per second speeds to handle the traffic from many computers;
- Optical fibers (versus copper wires) that provide high data transfer
20 rates, with host-to-ATM switch connections running at 100 or 155 Mbps (million bits per second);
- Fixed size cells, each of which includes 53 bytes.

ATM incorporates features of both packet switching and circuit switching, as
25 it is designed to carry voice, video, and television signals in addition to data.

Pure packet switching technology is not conducive to carrying voice transmissions because such transfers demand more stable bandwidth.

-41-

B. Frame Relay

Frame relay systems use packet switching techniques, but are more efficient than traditional systems. This efficiency is partly due to the fact that they perform less error checking than traditional X.25 packet-switching services.

- 5 In fact, many intermediate nodes do little or no error checking at all and only deal with routing, leaving the error checking to the higher layers of the system. With the greater reliability of today's transmissions, much of the error checking previously performed has become unnecessary. Thus, frame relay offers increased performance compared to traditional systems.

10

C. ISDN

An Integrated Services Digital Network is an "international telecommunications standard for transmitting voice, video, and data over digital lines," most commonly running at 64 kilobits per second. The traditional phone network runs voice at only 4 kilobits per second. To adopt ISDN, an end user or company must upgrade to ISDN terminal equipment, central office hardware, and central office software. The ostensible goals of ISDN include the following:

- 15 1. To provide an internationally accepted standard for voice, data and signaling;
- 20 2. To make all transmission circuits end-to-end digital;
3. To adopt a standard out-of-band signaling system; and

To bring significantly more bandwidth to the desktop.

VI. MCI INTELLIGENT NETWORK

- 25 The MCI Intelligent Network is a call processing architecture for processing voice, fax and related services. The Intelligent Network comprises a special purpose bridging switch with special capabilities and a set of general purpose computers along with an Automatic Call Distributor (ACD). The call processing including number translation services, automatic or manual
- 30 operator services, validation services and database services are carried out

-42-

on a set of dedicated general purpose computers with specialized software. New value added services can be easily integrated into the system by enhancing the software in a simple and cost-effective manner.

5 Before proceeding further, it will be helpful to establish some terms.

ISP	Intelligent Services Platform
NCS	Network Control System
DAP	Data Access Point
ACD	Automatic Call Distributor
10 ISN	Intelligent Services Network (Intelligent Network)
ISNAP	Intelligent Services Network Adjunct Processor
MTOC	Manual Telecommunications Operator Console
ARU	Audio Response Unit
ACP	Automatic Call Processor
15 NAS	Network Audio Server
EVS	Enhanced Voice Services
POTS	Plain Old Telephone System
ATM	Asynchronous Transfer Mode

20 The Intelligent Network Architecture has a rich set of features and is very flexible. Addition of new features and services is simple and fast. Features and services are extended utilizing special purpose software running on general purpose computers. Adding new features and services involves upgrading the special purpose software and is cost-effective.

25

Intelligent Network Features and Services include

- Call type identification;
- Call Routing and selective termination;
- Operator selection and call holding;
- 30 • Manual and Automated Operator;
- Voice Recognition and automated, interactive response;

-43-

- Customer and customer profile verification and validation;
- Voice Mail;
- Call validation and database;
- Audio Conference reservation;
- 5 • Video Conference reservation;
- Fax delivery and broadcasting;
- Customer Billing;
- Fraud Monitoring;
- Operational Measurements and Usage Statistics reporting; and
- 10 Switch interface and control.

A. Components of the MCI Intelligent Network

- Figure **19A** illustrates an Intelligent Network in accordance with a preferred embodiment. The MCI Intelligent Network is comprised of a large number of
- 15 components. Major components of the MCI Intelligent Network include the
- MCI Switching Network **2**
 - Network Control System (NCS)/Data Access Point(DAP) **3**
 - ISN - Intelligent Services Network **4**
 - EVS - Enhanced Voice Services **9**

20

1. MCI Switching Network

- The MCI switching network is comprised of special purpose bridging switches **2**. These bridging switches **2** route and connect the calling and the called parties after the call is validated by the intelligent services network **4**.
- 25 The bridging switches have limited programming capabilities and provide the basic switching services under the control of the Intelligent Services Network (ISN) **4**.

-44-

2. Network Control System/Data Access Point (NCS/DAP)

The NCS/DAP **3** is an integral component of the MCI Intelligent Network. The DAP offers a variety of database services like number translation and also provides services for identifying the switch ID and trunk ID of the terminating number for a call.

The different services offered by NCS/DAP **3** include:

- Number Translation for 800, 900, VNET Numbers;
- Range Restrictions to restrict toll calling options and advanced parametric routing including Time of Day, Day of Week/Month, Point of Origin and percentage allocation across multiple sites;
- Information Database including Switch ID and Trunk ID of a terminating number for a given call;
- Remote Query to Customer Databases;
- VNET/950 Card Validation Services; and
- VNET ANI/DAL Validation Services.

3. Intelligent Services Network (ISN) 4

The ISN **4** includes an Automatic Call Distributor (ACD) for routing the calls.

The ACD communicates with the Intelligent Switch Network Adjunct Processor (ISNAP) **5** and delivers calls to the different manual or automated agents. The ISN includes the ISNAP **5** and the Operator Network Center (ONC). ISNAP **5** is responsible for Group Select and Operator Selection for call routing. The ISNAP communicates with the ACD for call delivery to the different agents. The ISNAP is also responsible for coordinating data and voice for operator-assisted calls. The ONC is comprised of Servers, Databases and Agents including Live Operators or Audio Response Units (ARU) including Automated Call Processors (ACP)s, MTOCs and associated NAS **7**. These systems communicate with each other on an Ethernet LAN and provide a variety of services for call processing.

-45-

The different services offered by the ONC include:

- Validation Services including call-type identification, call verification and call restrictions if any;
- 5 • Operator Services, both manual and automated, for customer assistance;
- Database Services for a variety of database lookups;
- Call Extending Capabilities;
- Call Bridging Capabilities;
- Prompt for User Input; and
- 10 • Play Voice Messages.

4. Enhanced Voice Services (EVS) 9

Enhanced Voice Services offer menu-based routing services in addition to a number of value-added features. The EVS system prompts the user for an
15 input and routes calls based on customer input or offers specialized services for voice mail and fax routing. The different services offered as a part of the EVS component of the MCI Intelligent Network include:

- Play Customer Specific Voice Messages;
- Prompt for User Input;
- 20 • User Input based Information Access;
- Call Extending Capabilities;
- Call Bridging Capabilities;
- Audio Conference Capabilities;
- Call Transfer Capabilities;
- 25 • Record User Voice Messages;
- Remote Update of Recorded Voice; and
- Send/Receive Fax.

5. Additional Components

30 In addition to the above mentioned components, a set of additional

-46-

components are also architected into the MCI Intelligent Network. These components are:

- Intelligent Call Routing (ICR) services are offered for specialized call routing based on information obtained from the calling party either during the call or at an earlier time. Routing is also based on the knowledge of the physical and logical network layout. Additional intelligent routing services based on time of day, alternate routing based on busy routes are also offered.
- Billing is a key component of the MCI Intelligent Network. The billing component provides services for customer billing based on call type and call duration. Specialized billing services are additionally provided for value added services like the 800 Collect calls.
- Fraud Monitoring component is a key component of the MCI Intelligent Network providing services for preventing loss of revenue due to fraud and illegal usage of the network.
- Operational Measurements include information gathering for analysis of product performance. Analysis of response to advertising campaigns, calling patterns resulting in specialized reports result from operational measurements. Information gathered is also used for future product planning and predicting infrastructure requirements.
- Usage Statistics Reporting includes gathering information from operational databases and billing information to generate reports of usage. The usage statistics reports are used to study call patterns, load patterns and also demographic information. These reports are used for future product plans and marketing input.

B. Intelligent Network System Overview

The MCI Call Processing architecture is built upon a number of key components including the MCI Switch Network, the Network Control
5 System, the Enhanced Voice Services system and the Intelligent Services Network. Call processing is entirely carried out on a set of general purpose computers and some specialized processors thereby forming the basis for the MCI Intelligent Network. The switch is a special purpose bridging switch with limited programming capabilities and complex interface. Addition of
10 new services on the switch is very difficult and sometimes not possible. A call on the MCI Switch is initially verified if it needs a number translation as in the case of an 800 number. If a number translation is required, it is either done at the switch itself based on an internal table or the request is sent to the DAP which is a general purpose computer with software capable
15 of number translation and also determining the trunk ID and switch ID of the terminating number.

The call can be routed to an ACD which delivers calls to the various call processing agents like a live operator or an ARU. The ACD communicates
20 with the ISNAP which does a group select to determine which group of agents are responsible for this call and also which of the agents are free to process this call.

The agents process the calls received by communicating with the NIDS
25 (Network Information Distributed Services) Server which are the Validation or the Database Servers with the requisite databases for the various services offered by ISN. Once the call is validated by processing of the call on the server, the agent communicates the status back to the ACD. The ACD in turn dials the terminating number and bridges the incoming call with the
30 terminating number and executes a Release Link Trunk (RLT) for releasing the call all the way back to the switch. The agent also generates a Billing

-48-

Detail Record (BDR) for billing information. When the call is completed, the switch generates an Operation Services Record (OSR) which is later matched with the corresponding BDR to create total billing information. The addition of new value added services is very simple and new features can be added by additional software and configuration of the different computing systems in the ISP. A typical call flow scenario is explained below.

C. Call Flow Example

The Call Flow example illustrates the processing of an 800 Number Collect Call from phone **1** in Figure **19A** to phone **10**. The call is commenced when a calling party dials 1-800-COLLECT to make a collect call to phone **10** the Called Party. The call is routed by the Calling Party's Regional Bell Operating Company (RBOC), which is aware that this number is owned by MCI, to a nearest MCI Switch Facility and lands on an MCI switch **2**.

The switch **2** detects that it is an 800 Number service and performs an 800 Number Translation from a reference table in the switch or requests the Data Access Point (DAP) **3** to provide number translation services utilizing a database lookup.

The call processing is now delegated to a set of intelligent computing systems through an Automatic Call Distributor (ACD) **4**. In this example, since it is a collect call, the calling party has to reach a Manual or an Automated Operator before the call can be processed further. The call from the switch is transferred to an ACD **4** which is operational along with an Intelligent Services Network Adjunct Processor (ISNAP) **5**. The ISNAP **5** determines which group of Agents are capable of processing the call based on the type of the call. This operation is referred to as Group Select. The agents capable of call processing include Manual Telecommunications Operator Console (MTOC)s **6** or Automated Call Processors (ACP)s **7** with associated Network Audio Servers (NAS)s **7a**. The ISNAP **5** determines

-49-

which of the Agents is free to handle the call and routes the voice call to a specific Agent.

5 The Agents are built with sophisticated call processing software. The Agent gathers all the relevant information from the Calling Party including the telephone number of the Called Party. The Agent then communicates with the database servers with a set of database lookup requests. The database lookup requests include queries on the type of the call, call validation based on the telephone numbers of both the calling and the called parties and also
10 call restrictions, if any, including call blocking restrictions based on the called or calling party's telephone number. The Agent then signals the ISNAP-ACD combination to put the Calling Party on hold and dial the called party and to be connected to the Called Party. The Agent informs the called party about the Calling Party and the request for a Collect Call. The Agent
15 gathers the response from the Called Party and further processes the call.

If the Called Party has agreed to receive the call, the Agent then signals the ISNAP-ACD combination to bridge the Called Party and the Calling Party. The Agent then cuts a BDR which is used to match with a respective OSR
20 generated by the switch to create complete billing information. The ISNAP-ACD combination then bridges the Called Party and the Calling Party and then releases the line back to the switch by executing a Release Trunk (RLT). The Calling Party and the Called Party can now have a conversation through the switch. At the termination of the call by either party, the switch
25 generates a OSR which will be matched with the BDR generated earlier to create complete billing information for the call. If the Called Party declines to accept the collect call, the Agent signals the ACD-ISNAP combination to reconnect the Calling Party which was on hold back to the Agent. Finally, the Agent informs the Calling Party about the Called Party's response and
30 terminates the call in addition to generating a BDR.

MCI Intelligent Network is a scaleable and efficient network architecture for

-50-

call processing and is based on a set of intelligent processors with specialized software, special purpose bridging switches and ACD's. The Intelligent Network is an overlay network coexisting with the MCI Switching Network and is comprised of a large number of specialized processors interacting with the switch network for call processing. One embodiment of Intelligent Network is completely audio-centric. Data and fax are processed as voice calls with some specialized, dedicated features and value-added services.

In another embodiment, the Intelligent Network is adapted for newly emerging technologies, including POTS-based video-phones and internet telephony for voice and video. The following sections describe in detail the architecture, features and services based on the emerging technologies.

COMPATIBILITY OF ISN WITH EMERGING TECHNOLOGIES

The following sections describe in detail the architecture, features and services based on several emerging technologies, all of which can be integrated into the Intelligent Network.

VII. ISP FRAMEWORK

A. Background

The ISP is composed of several disparate systems. As ISP integration proceeds, formerly independent systems now become part of one larger whole with concomitant increases in the level of analysis, testing, scheduling, and training in all disciplines of the ISP.

1. Broadband Access

A range of high bandwidth services are supported by a preferred

-51-

embodiment. These include: Video on Demand, Conferencing, Distance Learning, and Telemedicine.

ATM (asynchronous transfer mode) pushes network control to the periphery of the network, obviating the trunk and switching models of traditional, circuit-based telephony. It is expected to be deployed widely to accommodate these high bandwidth services.

2. Internet Telephony System

The Internet and with it, the World Wide Web, offers easy customer access, widespread commercial opportunities, and fosters a new role for successful telecommunications companies. The ISP platform offers many features which can be applied or reapplied from telephony to the Internet. These include access, customer equipment, personal accounts, billing, marketing (and advertising) data or application content, and even basic telephone service.

The telecommunication industry is a major transmission provider of the Internet. A preferred embodiment which provides many features from telephony environments for Internet clients is optimal.

Figure **19F** is a block diagram of an internet telephony system in accordance with a preferred embodiment. A number of computers **1900**, **1901**, **1902** and **1903** are connected behind a firewall **1905** to the Internet **1910** via an Ethernet or other network connection. A domain name system **1906** maps names to IP addresses in the Internet **1910**. Individual systems for billing **1920**, provisioning **1922**, directory services **1934**, messaging services **1930**, such as voice messaging **1932** are all attached to the internet **1910** via a communication link. Another communication link is also utilized to facilitate communications to a satellite device **1940** that is used to communicate information to a variety of set top devices **1941-1943**. A web

-52-

server **1944** provides access for an order entry system **1945** to the Internet **1910**.

5 In an embodiment, the order entry system **1945** generates complete profile information for a given telephone number, including, name, address, fax number, secretary's number, wife's phone number, pager, business address, e-mail address, IP address and phonemail address. This information is maintained in a database that can be accessed by everyone on the network with authorization to do so. In an alternate embodiment, the order entry
10 system utilizes a web interface for accessing an existing directory service database **1934** to provide information for the profile to supplement user entered information.

The Internet **1910** is tied to the Public Switched Network (PSTN) **1960** via a
15 gateway **1950**. The gateway **1950** in a preferred embodiment provides a virtual connection from a circuit switched call in the PSTN **1960** and some entity in the Internet **1910**.

The PSTN **1960** has a variety of systems attached, including a direct-dial
20 input **1970**, a Data Access Point (DAP) **1972** for facilitating 800 number processing and Virtual NETwork (VNET) processing to facilitate for example a company tieline. A Public Branch Exchange (PBX) **1980** is also attached via a communication link for facilitating communication between the PSTN **1960** and a variety of computer equipment, such as a fax **1981**, telephone
25 **1982** and a modem **1983**. An operator **1973** can also optionally attach to a call to assist in placing a call or conference call coming into and going out of the PSTN **1960** or the internet **1910**.

Various services are attached to the PSTN through individual
30 communication links including an attachment to the Intelligent Services Network (ISN) **1990**, direct-dial plan **1991**, provisioning **1974**, order entry **1975**, billing **1976**, directory services **1977**, conferencing services **1978**,

-53-

and authorization / authentication services **1979**. All of these services can communicate between themselves using the PSTN **1960** and the Internet **1910** via a gateway **1950**. The functionality of the ISN **1990** and the **DAP 1972** can be utilized by devices attached to the Internet **1910**.

5

Figure **19G** is a block diagram of a Prioritizing Access/Router in accordance with a preferred embodiment. A prioritizing access router (PAR) is designed to combine the features of an internet access device and an Internet Protocol (IP) Router. It enables dial-up modem access to the internet by performing
10 essential modem and PPP/SLIP to IP and the reverse IP to PPP/SLIP conversion. It also analyzes IP packet source/destination addresses and UPD or TCP ports and selects appropriate outgoing network interfaces for each packet. Lastly, it uses a priority routing technique to favor packets destined for specific network interfaces over packets destined for other
15 network interfaces.

The design goal of the prioritizing access/router is to segregate real-time traffic from the rest of the best- effort data traffic on internet networks. Real-time and interactive multimedia traffic is best segregated from traffic
20 without real-time constraints at the access point to the internet, so that greater control over quality of service can be gained. The process that a prioritizing access/router utilizes is presented below with reference to Figure **19G**.

25 First, at **2010**, a computer dials up the PAR via a modem. The computer modem negotiates a data transfer rate and modem protocol parameters with the PAR modem. The computer sets up a Point to Point Protocol (PPP) session with the PAR using the modem to modem connection over a Public Switched Telephone Network (PSTN) connection.
30 The computer transfers Point-to-Point (PPP) packets to the PAR using the modem connection. The PAR modem **2010** transfers PPP packets to the PPP to IP conversion process **2020** via the modem to host processor interface

-54-

2080. The modem to host processor interface can be any physical interface presently available or yet to be invented. Some current examples are ISA, EISA, VME, SCbus, MVIP bus, Memory Channel, and TDM buses. There is some advantage in using a multiplexed bus such as the Time Division Multiplexing buses mentioned here, due to the ability to devote capacity for specific data flows and preserve deterministic behavior.

The PPP to IP conversion process **2020** converts PPP packets to IP packets, and transfers the resulting IP packets to the packet classifier **2050** via the process to process interface **2085**. The process to process interface can be either a physical interface between dedicated processor hardware, or can be a software interface. Some examples of process to process software interfaces include function or subroutine calls, message queues, shared memory, direct memory access (DMA), and mailboxes.

The packet classifier **2085** determines if the packet belongs to any special prioritized group. The packet classifier keeps a table of flow specifications, defined by

destination IP Address

source IP address

combined source/destination IP Address

combined destination IP Address/UDP Port

combined destination IP Address/TCP Port

combined source IP address/UDP Port

combined source IP Address/TCP Port

combined source IP Address and TCP or UDP port with destination IP address

combined destination IP Address and TCP or UDP port with source IP address

combined source IP Address and TCP or UDP port with destination IP address and TCP/UDP Port.

-55-

The packet classifier checks its table of flow specifications against the IP addresses and UDP or TCP ports used in the packet. If any match is found, the packet is classified as belonging to a priority flow and labeled as with a priority tag. Resource Reservation Setup Protocol techniques may be used
5 for the packet classifier step.

The packet classifier **2050** hands off priority tagged and non-tagged packets to the packet scheduler **2060** via the process to process interface (90). The process to process interface **2090** need not be identical to the process to
10 process interface **2085**, but the same selection of techniques is available. The packet scheduler **2060** used a priority queuing technique such as Weighted Fair Queueing to help ensure that prioritized packets (as identified by the packet classifier) receive higher priority and can be placed on an outbound network interface queue ahead of competing best-effort traffic.

15

The packet scheduler **2060** hands off packets in prioritized order to any outbound network interface (**2010**, **2070**, **2071** or **2072**) via the host processor to peripheral bus **2095**. Any number of outbound network interfaces may be used.

20

IP packets can arrive at the PAR via non-modem interfaces (**2070**, **2071** and **2072**). Some examples of these interfaces include Ethernet, fast Ethernet, FDDI, ATM, and Frame Relay. These packets go through the same steps as IP packets arriving via the modem PPP interfaces.

25

The priority flow specifications are managed through the controller process **2030**. The controller process can accept externally placed priority reservations through the external control application programming interface **2040**. The controller validates priority reservations for particular flows
30 against admission control procedures and policy procedures, and if the reservation is admitted, the flow specification is entered in the flow specification table in the packet classifier **2050** via the process to process

-56-

interface **2065**. The process to process interface **2065** need not be identical to the process to process interface **2085**, but the same selection of techniques is available.

5 Turning now to Figure **20**, there is shown an architectural framework for an Intelligent Services Platform (ISP) **2100**, used in the present invention. The architecture of the ISP **2100** is intended to define an integrated approach to the provision and delivery of intelligent services to the MCI network across all the components of the ISP.

10

Each of the existing communication network systems has its own way of providing service management, resource management, data management, security, distributed processing, network control, or operations support.

15 The architecture of the ISP **2100** defines a single cohesive architectural framework covering these areas. The architecture is focused on achieving the following goals:

- Develop global capabilities;
- Deliver enhanced future services;
- Make efficient use of resources;
- 20 • Improve time to market;
- Reduce maintenance and operations costs;
- Increase overall product quality; and
- Introduce scalability both upward and downward capabilities.

25 The target capabilities of the ISP **2100** are envisioned to provide the basic building blocks for very many services. These services are characterized as providing higher bandwidth, greater customer control or personal flexibility, and much reduced , even instantaneous, provisioning cycles.

30 3. Capacity

The ISP **2100** has a reach that is global and ubiquitous. Globally, it will

-57-

reach every country through alliance partners' networks. In breadth, it reaches all business and residential locales through wired or wireless access.

5 4. Future Services

The above capabilities will be used to deliver:

- Telephony and messaging services beyond what we have today;
- Emerging video and multi-media offerings;
- Powerful data services, including enhanced private networks; and
- 10 • Software and equipment to enable end users to gain complete control over their services.

Services provided by the ISP **2100** will span those needed in advertising, agriculture, education, entertainment, finance, government, law,

15 manufacturing, medicine, network transmission, real estate, research, retailing, shipping, telecommunications, tourism, wholesaling, and many others.

Services:

- 20 • Customizable: customer is able to tailor the service offerings to their own needs.
- Customer managed: customer has direct (network-side) access for the administration and control of their service.
- Loosely Coupled: services obtain and use network resources only
- 25 when needed; customers pay for only what they use. Bandwidth is available on demand, and without pre-allocation.
- Secure & Private: customer privacy and confidentiality is paramount in the networked world. Commercial interests are guaranteed safe, secure transactions. Users and customers are identified and
- 30 authenticated, and the network protected from tampering or corruption.

B. ISP Architecture Framework

The following section describes the role of the ISP Platform **2100** in providing customer services.

5

The ISP **2100** provides customer services through an intelligent services infrastructure, including provider network facilities **2102**, public network facilities **2104**, and customer equipment **2106**. The services infrastructure ensures the end-to-end quality and availability of customer service.

10

The following section describes the relationship of the ISP platform **2100** to various external systems both within and outside a provider.

The provider components **2108** in Figure **20** are:

- 15 • Intelligent Services **2110** - responsible for service provisioning, service delivery, and service assurance, including the internal data communications networks **2102**. This represents the ISP's role.
- Revenue Management **2112** - responsible for financial aspects of customer services.
- 20 • Network Management **2114** - responsible for the development and operation of the physical networks **2102**.
- Product Management **2116** - responsible for the creation and marketing of customer services.

The entities external to the ISP **2100** depicted in Figure **20** are:

- 25 • Networks **2104**- this represents all the network connections and access methods used by customers 2106 for service. This includes a provider's circuit switched network, packet switched networks, internal extended wide area network, the internet, a provider's wireless partners' networks, a provider's global alliance and national partner networks, broadband
- 30 networks, as well as the customer premises equipment **2118** attached to these networks.

-59-

- 3rd party Service Providers **2120** - this represents those external organizations which deliver services to customers via the provider's Intelligent Services Platform **2100**.
- Service Resellers **2122** - this represents those organizations which have customers using the facilities **2100**.
- Global Alliance Partners **2124** - organizations which have shared facilities and exchange capabilities of their networks and service infrastructures.

C. *ISP Functional Framework*

- Figure **21** shows components of the ISP **2100** in more detail. Shown is the set of logical components comprising the ISP **2100** architecture. None of these components is a single physical entity; each typically occurs multiple times in multiple locations. The components work together to provide a seamless Intelligent Services **2110** environment. This environment is not fixed; it is envisioned as a flexible evolving platform capable of adding new services and incorporating new technologies as they become available. The platform components are linked by one or more network connections which include an internal distributed processing infrastructure.
- The ISP **2100** Functional Components are:
- Inbound and Outbound Gateways **2126** - allows access to services provided by other providers, and allows other providers to access the provider's services.
 - Marketable Service Gateway **2128**- interface to a three-tier service creation environment for services the provider sells. Services are deployed and updated through the Marketable Service Gateway **2128**. This is actually no different than the Management Service Gateway **2130**, except that the services created and deployed through here are for external customers.
 - Management Service Gateway **2130** - illustrates that service creation concepts apply to management of the platform as well as service logic.

-60-

Management services are deployed and managed through the Management Service Gateway **2130**. Also, interfaces with management systems external to ISP **2100** are realized by the Management Service Gateway **2130**. Some examples of management services include the collection, temporary storage, and forwarding of (billable) network events. Other services include collection and filtering of alarm information from the ISP **2100** before forwarding to network management **2132**.

• Service Engines **2134** - A Service Logic Execution Environment for either marketable or management services. The Service Engines **2134** execute the logic contained in customer-specific profiles in order to provide unique customized service features.

• Service Creation Environment **2136** - Creates and deploys management services as well as marketable services, and their underlying features and capabilities.

• Data Management **2138** - Where all customer and service profile data is deployed. Data is cached on Service Engines **2134**, Statistics Servers **2140**, Call Context servers **2142**, Analysis Servers **2144**, and other specialized applications or servers **2146** requiring ISP **2100** data.

• Service Select **2148** - Whether the services are accessed via a narrowband or broadband network, circuit-switched, packet-switched, or cell-switched, the services are accessed via a Service Select function **2148**. Service Select **2148** is a specialized version of a service engine **2134**, designed specifically to choose a service or services to execute.

• Resource Managers **2150** - manages all resources, including specialized resources **2152** and service instances running on service engines **2134**, and any other kind of resource in the ISP **2100** that needs management and allocation.

-61-

• Specialized Resources **2152** - Special network-based capabilities (Internet to voice conversion, DTMF-detection, Fax, Voice Recognition, etc) are shown as specialized resources **2152**.

5

• Call Context Server **2142** - accepts network event records and service event records in real time, and allows queries against the data. Once all events for a call (or any other kind of network transaction) are generated, the combined event information is delivered en masse to the Revenue Management

10 function **2154**. Data is stored short-term.

• Statistics Server **2140**- accepts statistics events from service engines, performs rollups, and allows queries against the data. Data is stored short-term.

15

• Customer Based Capabilities **2156**- software and specialized hardware on the customer premises that enables customer-premises based capabilities, such as ANI screening, Internet access, compression, interactive gaming, videoconferencing, retail access, you name it.

20

• Analysis Services **2144**- a special kind of service engine that isn't based on network access, but is based on adding value based upon network statistics or call context information in real time or near real time. Examples include fraud detection and customer traffic statistics.

25

• Other Special Services **2146**- entail other specialized forms of applications or servers that may or may not be based on the Service Engine model. These components provide other computing resources and lower-level functional capabilities which may be used in Service delivery, monitoring, or

30 management.

-62-

D. ISP Integrated Network Services

Figure **22** shows how the ISP architecture **2100** supplies services via different networks. The networks shown include Internet **2160**, the public switched telephony network (PSTN) **2162**, Metro access rings **2164**, and
5 Wireless **2166**. Additionally, it is expected that new "switchless" broadband network architectures **2168** and **2170** such as ATM or ISOEthernet may supplant the current PSTN networks **2162**.

10 The architecture accommodates networks other than basic PSTNs **2162** due to the fact that these alternative network models support services which cannot be offered on a basic PSTN, often with an anticipated reduced cost structure. These Networks are depicted logically in Figure **22**.

Each of these new networks are envisioned to interoperate with the ISP
15 **2100** in the same way. Calls (or transactions) will originate in a network from a customer service request, the ISP will receive the transaction and provide service by first identifying the customer and forwarding the transaction to a generalized service-engine **2174**. The service engine determines what service features are needed and either applies the
20 necessary logic or avails itself of specialized network resources for the needed features.

The ISP **2100** itself is under the control of a series of Resource managers and Administrative and monitoring mechanisms. A single system image is
25 enabled through the concurrent use of a common information base. The information base holds all the Customer, Service, Network and Resource information used or generated by the ISP. Other external applications (from within MCI and in some cases external to MCI) are granted access through gateways, intermediaries, and sometimes directly to the same information
30 base.

-63-

In Figure **22**, each entity depicts a single logical component of the ISP. Each of these entities is expected to be deployed in multiple instances at multiple sites.

5 **E. ISP Components**

Ext App **2176**- an external application;

App **2178**- an internal ISP application (such as Fraud Analysis);

Dc **2180**- Data client, a client to the ISP information base which provides a local data copy;

10 Ds **2182**- Data server, one of the master copies of ISP information;

Admin **2184**- the ISP administrative functions (for configurations, and maintenance);

Mon **2186**- the ISP monitoring functions (for fault, performance, and accounting);

15 GRM **2188**- the global resource management view for selected resources;

LRM **2190**- the local resource management view for selected resources;

SR **2192**- the pools of specialized resources (such as video servers, ports, speech recognition);

SE **2134**- the generalized service engines which execute the desired service logic; and

20 Service Select **2194**- the function which selects the service instance (running on a service engine **2134**) which should process transactions offered from the networks.

25 **F. Switchless Communications Services**

The switchless network **2168** is a term used for the application of cell-switching or packet-switching techniques to both data and isochronous multimedia communications services. In the past, circuit switching was the only viable technology for transport of time-sensitive isochronous voice.

30 Now, with the development of Asynchronous Transfer Mode cell switching

-64-

networks which provide quality of service guarantees, a single network infrastructure which serves both isochronous and bursty data services is achievable.

- 5 The switchless network is expected to provide a lower cost model than circuit switched architectures due to:
- Flexibility to provide exactly the bandwidth required for each application, saving bandwidth when no data is being transferred. A minimum 56 Kbps circuit will not automatically be allocated for every call.
 - 10 • Adaptability to compression techniques, further reducing bandwidth requirements for each network session.
 - Lower costs for specialized resource equipment, due to the fact that analog ports do not have to be supplied for access to special DSP capabilities such as voice recognition or conferencing. A single high-bandwidth network port
 - 15 can serve hundreds of "calls" simultaneously.
 - Applicability and ease of adaptation of the switchless networks to advanced high-bandwidth services such as videoconferencing, training on demand, remote expert, integrated video/voice/fax/electronic mail, and information services. Figure **23** illustrates a sample switchless network **2168** in
 - 20 accordance with a preferred embodiment.

G. Governing Principles

1. Architectural Principles

This section contains a listing of architectural principles which provide the foundation of the architecture which follows.

Service Principles

1. The Service Model must support seamless integration of new and existing services.
2. Services are created from a common Service Creation Environment (SCE) which provides a seamless view of services.

-65-

3. All services execute in common service logic execution environments (SLEEs), which do not require software changes when new services are introduced.
4. All services are created from one or more service features.
- 5 5. Data stored in a single customer profile in the ISP Data Servers may be used to drive multiple services.
6. The Service Model must support the specification and fulfillment of quality of service parameters for each service. These quality of service parameters, when taken together, constitute a service level agreement
10 with each customer. Service deployment must take into account specified quality of service parameters.

2. Service Feature Principles

- 15 1. All service features are described by a combination of one or more capabilities.
2. All service features can be defined by a finite number of capabilities.
3. Individual service features must be defined using a standard methodology to allow service designers to have a common understanding of a capability. Each service feature must document
20 their inputs, outputs, error values, display behaviors, and potential service applications.
4. Interaction of physical entities in the network implementation shall not be visible to the user of the service feature through the service feature interfaces.
- 25 5. Each service feature should have a unified and stable external interface. The interface is described as a set of operations, and the data required and provided by each operation.
6. Service features are not deployed into the network by themselves. A service feature is only deployed as part of a service logic program
30 which invokes the service feature (see Figure 21). Thus, service features linked into service logic programs statically, while capabilities

-66-

are linked to service logic programs dynamically. This is where the loose coupling of resources to services is achieved.

3. Capability Principles

- 5 1. Capabilities are defined completely independent from consideration of any physical or logical implementation (network implementation independent).
2. Each capability should have a unified and stable interface. The interface is described as a set of operations, and the data required and
10 provided by each operation.
3. Individual capabilities must be defined using a standard methodology to allow service designers to have a common understanding of a capability. Each capability must document their inputs, outputs, error values, display behaviors, and potential service
15 applications.
4. Interaction of physical entities in the network implementation shall not be visible to the user of the capability through the capability interfaces.
5. Capabilities may be combined to form high-level capabilities.
- 20 6. An operation on a capability defines one complete activity. An operation on a capability has one logical starting point and one or more logical ending points.
7. Capabilities may be realized in one or more piece of physical hardware or software in the network implementation.
- 25 8. Data required by each capability operation is defined by the capability operation support data parameters and user instance data parameters.
9. Capabilities are deployed into the network independent of any service.
- 30 10. Capabilities are global in nature and their location need not be considered by the service designer, as the whole network is regarded

-67-

as a single entity from the viewpoint of the service designer.

11. Capabilities are reusable. They are used without modification for other services.

5 4. Service Creation, Deployment, and Execution Principles

1. Each Service Engine **2134** supports a subset of the customer base. The list of customers supported by a service engine is driven by configuration data, stored on the ISP Data Server **2182**.
2. Each Service Engine **2134** obtains its configuration data from the
10 ISP data servers **2152** at activation time.
3. Service Engines **2134** use ISP database clients **2180** (see the data management section of this description) to cache the data necessary to support the customers configured for that service engine **2134**, as needed. Caching can be controlled by the ISP database server **2182**,
15 or controlled by the database of the ISP database server **2182**. Data may be cached semi-permanently (on disk or in memory) at a service engine **2134** if it is deemed to be too much overhead to load data from the data server **2182** on a frequent basis.
4. Service Engines **2134** may be expected to execute all of a customer's
20 services, or only a subset of the customer's services. However, in the case of service interactions, one Service Engine **2134** must always be in control of the execution of a service at any given time. Service Engines may hand-off control to other service engines during the course of service execution.
- 25 5. Service Engines do not own any data, not even configuration data.
6. Service Engines **2134** are not targets for deployment of data. Data Servers **2182** are targets for deployment of data.

5. Resource Management Model **2150** Principles

- 30 1. Resources **2152** should be accessible from anywhere on the network.

-68-

2. Resources are not service-specific and can be shared across all services if desired.
3. Resources of the same type should be managed as a group.
4. The Resource Management Model **2150** should be flexible enough to
5 accommodate various management policies, including: Least Cost, Round Robin, Least Recently Used, Most Available, First Encountered, Use Until Failure and Exclusive Use Until Failure.
5. The Resource Management Model **2150** should optimize the allocation of resources and, if possible, honoring a selected policy.
- 10 6. The RM **2150** must allow for a spectrum of resource allocation techniques ranging from static configuration to fully dynamic allocation of resources on a transaction by transaction basis.
7. The Resource Management Model **2150** must allow for the enforcement of resource utilization policies such as resource time out
15 and preemptive reallocation by priority.
8. The Resource Management Model **2150** must be able to detect and access the status, utilization and health of resources in a resource pool.
9. All Resources **2152** must be treated as managed objects.
- 20 10. All resources must be able to register with the RM **2150** to enter a pool, and de-register to leave a pool.
11. The only way to request, acquire and release a resource **2152** is through the RM **2150**.
12. The relationship between resources should not be fixed, rather
25 individual instances of a given resource should be allocated from a registered pool in response to need or demand.
13. All specialized resources **2152** must be manageable from a consistent platform-wide viewpoint.
14. All specialized resources **2152** must offer SNMP or CMIP agent
30 functionality either directly or through a proxy.
15. Every specialized resource **2152** shall be represented in a common management information base.

-69-

16. All specialized resources shall support a standard set of operations to inquire, probe, place in or out of service, and test the item.
17. All specialized resources shall provide a basic set of self-test capabilities which are controlled through the standard SNMP or CMIP management interfaces.

6. Data Management **2138** Principles

1. Multiple copies of any data item are allowed.
2. Multiple versions of the value of a data item are possible, but one view is considered the master.
3. Master versions of a given data item are under a single jurisdiction.
4. Multiple users are allowed to simultaneously access the same data.
5. Business rules must be applied uniformly across the ISP 2100 to ensure the validity of all data changes.
6. Users work on local copies of data; data access is location independent and transparent.
7. From the data management point of view, users are applications or other software components.
8. Data access should conform to a single set of access methods which is standardized across the ISP **2100**.
9. Private data is allowed at a local database, but cannot be shared or distributed.
10. Only master data can be shared or distributed.
11. Private formats for a shared data item are allowed at the local database.
12. Transactional capabilities can be relaxed at end-user discretion if allowed within the business rules.
13. Rules-based logic and other meta-data controls provide a flexible means to apply policy.
14. Data Replication provides reliability through duplication of data sources.

-70-

15. Database Partitioning provides scalability by decreasing the size of any particular data store, and by decreasing the transaction rate against any particular data store.
16. Data Management **2138** must allow both static and dynamic configuration of data resources.
17. Common data models and common schemas should be employed.
18. Logical application views of data are insulated from physical data operations such as relocation of files, reloading of databases, or reformatting of data stores.
19. Audit trails, and event histories, are required for adequate problem resolutions.
20. On-line data audits and reconciliation are required to ensure data integrity.
21. Data recovery of failed databases is needed in real time.
22. Data metrics are needed for monitoring, trending, and control purposes.
23. 7 by 24 operation with 99.9999 availability is required.
24. Data Management **2138** mechanisms must scale for high levels of growth.
25. Data Management **2138** mechanisms must provide cost effective solutions for both large-scale and small-scale deployments.
26. Data Management mechanisms must handle overload conditions gracefully.
27. Data processing and data synchronization must occur in real-time to meet our business needs.
28. Trusted order entry and service creation should work directly on the ISP databases rather than through intermediary applications whenever possible.
29. All data must be protected; additionally customer data is private and must retain its confidentiality.
30. Configurations, operational settings, and run-time parameters are mastered in the ISP MIB (management information base).

-71-

31. Wherever possible, off the shelf data solutions should be used to meet Data Management needs.

The following principles are stated from an Object-oriented view:

- 5 32. Data items are the lowest set of persistent objects; these objects encapsulate a single data value.
33. Data items may have a user defined type.
34. Data items may be created and deleted.
35. Data items have only a single get and set method.
- 10 36. The internal value of a data item is constrained by range restrictions and rules.
37. Data items in an invalid state should be inaccessible to users.

7. Operational Support Principles

- 15 1. Common View - All ISP **2100** Operational Support User Interfaces should have the same look & feel.
2. Functional Commonality - The management of an object is represented in the same manner throughout the ISP Operational support environment.
- 20 3. Single View - A distributed managed object has a single representation at the ISP Operational Support User Interfaces, and the distribution is automatically.
4. OS/DM Domain - Data within the Operational support domain should be managed with the ISP Data Management **2138** Mechanisms.
- 25 5. Global MIB - There is a logical Global MIB which represents resources in the entire ISP.
6. External MIBs - Embedded MIBs that are part of a managed component are outsider of Operational Support and Data Management. Such MIBs will be represented to the OS by a Mediation
- 30 Device.
7. System Conformance - System conformance to the ISP OS standards

-72-

will be gained through Mediation Layers.

8. Operational Functions - Operational personnel handle the Network Layer & Element Management for physical & logical resources.
9. Administration Functions - Administration personnel handle the Planning & Service Management.
10. Profile Domain - Service & customer profile data bases are managed by administration personnel under the domain of the Data Management system.
11. Telecommunication Management Network (TMN) compliance - TMN compliance will be achieved through a gateway to any TMN system.
12. Concurrent - Multiple Operators & Administrators must be able to simultaneously perform operations from the ISP OS Interfaces.

8. Physical Model Principles

1. Compatibility: The physical network model provides backward compatibility for existing telecommunications hardware and software.
2. Scaleable: The physical network model is scaleable to accommodate a wide range of customer populations and service requirements.
3. Redundant: The physical network model provides multiple paths of information flow across two network elements. Single points of failure are eliminated.
4. Transparent: Network elements is transparent to the underlying network redundancy. In case of a failure, the switchover to redundant links is automatic.
5. Graceful Degradation: The physical network model is able to provide available services in a gradual reduction of capacity in the face of multiple network failures.
6. Interoperable: The physical network model allows networks with different characteristics to interoperate with different network elements.
7. Secure: The physical network model requires and provides secure

-73-

transmission of information. It also has capabilities to ensure secure access to network elements.

8. Monitoring: The physical network model provides well-defined interfaces and access methods for monitoring the traffic on the network. Security (see above) is integrated to prevent unauthorized access to sensitive data.
9. Partitionable: The physical network model is (logically) partitionable to form separate administrative domains.
10. Quality of Service: The physical network model provides QOS provisions such as wide range of qualities, adequate QOS for legacy applications, congestion management and user-selectable QOS.
11. Universal Access: The physical network model does not prevent access to a network element due to its location in the network. A service is able to access any resource on the network.
12. Regulatory awareness: The physical network model is amenable at all levels to allow for sudden changes in the regulatory atmosphere.
13. Cost Effective: The physical network model allows for cost effective implementations by not being reliant on single vendor platforms or specific standards for function.

H. ISP Service Model

This section describes the Service model of the Intelligent Services Platform Architecture Framework.

1. Purpose

The ISP Service Model establishes a framework for service development which supports:

- rapid service creation and deployment;
- efficient service execution;
- complete customization control over services for customers;

-74-

- total service integration for a seamless service view for customers;
- improved reuse of ISP capabilities through loose coupling of those capabilities;
- reduced cost of service implementation; and
- 5 • vendor-independence.

2. Scope of Effort

The ISP Service Model supports all activities associated with Services, including the following aspects:

- 10 • provisioning;
- creation;
- deployment;
- ordering;
- updating;
- 15 • monitoring;
- execution;
- testing or simulation;
- customer support and troubleshooting;
- billing;
- 20 • trouble ticket handling; and
- operations support.

This model covers both marketable services and management services.

- Marketable services are the services purchased by our customers
- 25 • Management services are part of the operation of the MCI network, and are not sold to customers.

The Service Model also defines interactions with other parts of the ISP Architecture, including Data Management, Resource Management, and

30 Operational Support.

3. Service Model Overview

Central to the Intelligent Services Platform is the delivery of Services **2200** (Figure **24**). Services are the most critical aspect in a telecommunication service provider's ability to make money. The following definition of services is used throughout this service model:

A service **2200** is a set of capabilities combined with well-defined logic structures and business processes which, when accessed through a published interface, results in a desired and expected outcome on behalf of the user.

One of the major differences between a Service **2200** and an Application **2176** or **2178** (Figure **22**) is that a Service **2200** includes the business processes that support the sale, operation, and maintenance of the Service. The critical task in developing a Service is defining what can be automated, and clearly delineating how humans interact with the Service.

4. Service Structure

The vocabulary we will use for describing services includes the services themselves, service features, and capabilities. These are structured in a three-tier hierarchy as shown in Figure **24**.

A service **2200** is an object in a sense of an object-oriented object as described earlier in the specification. An instance of a service **2200** contains other objects, called service features **2202**. A service feature **2202** provides a well defined interface which abstracts the controlled interaction of one or more capabilities **2204** in the ISP Service Framework, on behalf of a service.

Service features **2202**, in turn, use various capability **2204** objects.

Capabilities **2204** are standard, reusable, network-wide building blocks used to create service features **2202**. The key requirement in Service

-76-

Creation is for the engineers who are producing basic capability objects to insure each can be reused in many different services as needed.

a) Services 2200

Services **2200** are described by "service logic," which is basically a program written in a very high-level programming language or described using a graphical user interface. These service logic programs identify:

- what service features **2202** are used;
- the order in which service features are invoked;
- the source of input service data;
- the destination for output service data;
- error values and error handling;
- invocation of other services **2200**;
- interaction with other services; and
- the interactions with other services;

The service logic itself is generally not enough to execute a service **2200** in the network. Usually, customer data is needed to define values for the points of flexibility defined in a service, or to customize the service for the customer's particular needs. Both Management and Marketable Services are part of the same service model. The similarities between of Management and Marketable Services allow capabilities to be shared. Also, Management and Marketable Services represent two viewpoints of the same network: Management Services represent an operational view of the network, and Marketable Services represent an external end-user or customer view of the network. Both kinds of services rely on network data which is held in common.

Every Marketable Service has a means for a customer to order the service, a billing mechanism, some operational support capabilities, and service monitoring capabilities. The Management Services provide processes and supporting capabilities for the maintenance of the platform.

-77-

b) Service Features 2202

Service features **2202** provide a well-defined interface of function calls.

Service features can be reused in many different services **2200**, just as

5 capabilities **2204** are reused in many different service features **2202**.

Service features have specific data input requirements, which are derived from the data input requirements of the underlying capabilities. Data output behavior of a service feature is defined by the creator of the service feature, based upon the data available from the underlying capabilities.

10 Service Features **2202** do not rely on the existence of any physical resource, rather, they call on capabilities **2204** for these functions, as shown in Figure **25**.

Some examples of service features are:

15 •Time-based Routing - based on capabilities such as a calendar, date/time, and call objects, this feature allows routing to different locations based upon time.

•Authentication - based upon capabilities such as comparison and database lookup, this function can be used to validate calling card use by
20 prompting for a card number and/or an access number (pin number), or to validate access to a virtual private network.

•Automated User Interaction - based upon capabilities such as voice objects (for recording and playback of voice), call objects (for transferring and bridging calls to specialized resources), DTMF objects (for collection or
25 outpulsing of DTMF digits), vocabulary objects (for use with speech recognition), this feature allows automated interaction with the user of a service. This service feature object can be extended to include capabilities for video interaction with a user as well.

-78-

c) Capabilities 2204

A capability **2204** is an object, which means that a capability has internal, private state data, and a well-defined interface for creating, deleting, and using instances of the capability. Invoking a capability **2204** is done by
5 invoking one of its interface operations. Capabilities **2204** are built for reuse. As such, capabilities have clearly defined data requirements for input and output structures. Also, capabilities have clearly defined error handling routines.

Capabilities may be defined in object-oriented class hierarchies whereby a
10 general capability may be inherited by several others.

Some examples of network-based capability objects are:

- voice (for recording or playback),
- call (for bridging, transferring, forwarding, dial-out, etc),
- 15 • DTMF (for collection or outpulsing), and
- Fax (for receive, send, or broadcast).

Some capabilities are not network-based, but are based purely on data that has been deployed into our platform. Some examples of these capabilities
20 are:

- calendar (to determine what day of the week or month it is),
- comparison (to compare strings of digits or characters),
- translation (to translate data types to alternate formats), and
- distribution (to choose a result based on a percentage distribution).

d) Service Data

There are three sources for data while a service executes:

- Static Data defined in the service template, which include default values for a given service invocation.
- 30 • Interactive Data obtained as the service executes, which may be

-79-

explicit user inputs or derived from the underlying network connections.

- Custom Data defined in User Profiles, which is defined by customers or their representatives when the service is requested (i.e. at creation time).

5. Service **2200** Execution

Services **2200** execute in Service Logic Execution Environments (SLEEs). A SLEE is executable software which allows any of the services deployed into the ISP **2100** to be executed. In the ISP Architecture, Service Engines **2134** (Figure **21**) provide these execution environments. Service Engines **2134** simply execute the services **2200** that are deployed to them.

Service templates and their supporting profiles are deployed onto database servers **2182** (Figure **22**). When a SLEE is started on a Service Engine **2134**, it retrieves its configuration from the database server **2182**. The configuration instructs the SLEE to execute a list of services **2200**. The software for these services is part of the service templates deployed on the database servers. If the software is not already on the Service Engine **2134**, the software is retrieved from the database server **2182**. The software is executed, and service **200** begins to run.

In most cases a service **2200** will first invoke a service feature **2202** (Figure **24**) which allows the service to register itself with a resource manager **2188** or **2190**. Once registered, the service can begin accepting transactions. Next, a service **2200** will invoke a service feature **2202** which waits on an initiating action. This action can be anything from an internet logon, to an 800 call, to a point of sale card validation data transaction. Once the initiating action occurs in the network, the service select function **2148** (Figure **21**) uses the Resource Manager **2150** function to find an instance of the executing service **2200** to invoke. The initiating action is delivered to

-80-

the service **2200** instance, and the service logic (from the service template) determines subsequent actions by invoking additional service features **2202**.

5 During service **2200** execution, profile data is used to determine the behavior of service features **2202**. Depending on service performance requirements, some or all of the profile data needed by a service may be cached on a service engine **2134** from the ISP **2100** database server **2182** to prevent expensive remote database lookups. As the service executes,
10 information may generated by service features **2202** and deposited into the Context Database. This information is uniquely identified by a network transaction identifier. In the case of a circuit-switched call, the already-defined Network Call Identifier will be used as the transaction identifier. Additional information may be generated by network equipment and
15 deposited into the Context Database as well, also indexed by the same unique transaction identifier. The final network element involved with the transaction deposits some end-of-transaction information into the Context Database. A linked list strategy is used for determining when all information has been deposited into the Context Database for a particular transaction.
20 Once all information has arrived, an event is generated to any service which has subscribed to this kind of event, and services may then operate on the data in the Context Database. Such operations may include extracting the data from the Context Database and delivering it to billing systems or fraud analysis systems.

25

6. Service Interactions

In the course of a network transaction, more than one service can be invoked by the network. Sometimes, the instructions of one service may conflict with the instructions of another service. Here's an example of such
30 a conflict: a VNET caller has a service which does not allow the caller to place international calls. The VNET caller dials the number of another VNET

-81-

user who has a service which allows international dialing, and the called VNET user places an international call, then bridges the first caller with the international call. The original user was able to place an international call through a third party, in defiance of his company's intention to prevent the user from dialing internationally. In such circumstances, it may be necessary to allow the two services to interact with each other to determine if operation of bridging an international call should be allowed.

The ISP service model must enable services **2200** to interact with other services. There are several ways in which a service **2200** must be able to interact with other services (see Figure **26**):

- Transfer of Control **2210**: where a service has completed its execution path and transfers control to another service;
- Synchronous Interaction **2212**: where a service invokes another service and waits for a reply;
- Asynchronous Interaction **2214**: where a service invokes another service, performs some other actions, then waits for the other service to complete and reply; or
- One Way Interaction **2216**: where a service invokes another service but does not wait for a reply.

In the example of interacting VNET services above, the terminating VNET service could have queried the originating VNET service using the synchronous service interaction capability. The interesting twist to this idea is that service logic can be deployed onto both network-based platforms and onto customer premises equipment. This means that service interaction must take place between network-based services and customer-based services.

7. Service Monitoring

Services **2200** must be monitored from both the customer's viewpoint and

-82-

the network viewpoint. Monitoring follows one of two forms:

- The service **2200** can generate detailed event-by-event information for delivery to the transaction context database
 - The service can generate statistical information for delivery periodically to a statistics database, or for retrieval on demand by a statistics database.
- Analysis services can use the Statistics Database or the Context Database to perform real time or near real time data analysis services.

The Context Database collects all event information regarding a network transaction. This information will constitute all information necessary for network troubleshooting, billing, or network monitoring.

I. ISP Data Management Model

This section describes the Data Management **2138** aspects of the Intelligent Services Platform (ISP) **2100** Target Architecture.

1. Scope

The ISP Data Management **2138** Architecture is intended to establish a model which covers the creation, maintenance, and use of data in the production environment of the ISP **2100**, including all transfers of information across the ISP boundaries.

The Data Management **2138** Architecture covers all persistent data, any copies or flows of such data within the ISP, and all flows of data across the ISP boundaries. This model defines the roles for data access, data partitioning, data security, data integrity, data manipulation, plus database administration. It also outlines management policies when appropriate.

2. Purpose

The objectives of this architecture are to:

-83-

- Create a common ISP functional model for managing data;
- Separate data from applications;
- Establish patterns for the design of data systems;
- Provide rules for systems deployment;
- 5 • Guide future technology selections; and
- Reduce redundant developments and redundant data storage.

Additional goals of the target architecture are:

- Ensure data flexibility;
- 10 • Facilitate data sharing;
- Institute ISP-wide data control and integrity;
- Establish data security and protection;
- Enable data access and use;
- Provide high data performance and reliability;
- 15 • Implement data partitioning; and
- Achieve operational simplicity.

3. Data management Overview

In one embodiment, the Data Management Architecture is a framework
20 describing the various system components, how the systems interact, and
the expected behaviors of each component. In this embodiment data is
stored at many locations simultaneously, but a particular piece of data and
all of its replicated copies are viewed logically as a single item. A key
difference in this embodiment is that the user (or end-point) dictates what
25 data is downloaded or stored locally.

a) Domains

Data and data access are characterized by two domains **2220** and **2222**, as
shown in Figure **27**. Each domain can have multiples copies of data within
30 it. Together, the domains create a single logical global database which can

-84-

span international boundaries. The key aspect to the domain definitions below is that all data access is the same. There is no difference in an Order Entry feed from a Call Processing lookup or Network side data update.

- 5 Central domain **2220** controls and protects the integrity of the system. This is only a logical portrayal, not a physical entity. Satellite domain **2222** provides user access and update capabilities. This is only a logical portrayal, not a physical entity.

10

b) Partitions

- In general, Data is stored at many locations simultaneously. A particular piece of data and all of its replicated copies are viewed logically as a single item. Any of these copies may be partitioned into physical subsets so that
- 15 not all data items are necessarily at one site. However partitioning preserves the logical view of only one, single database.

c) Architecture

- The architecture is that of distributed databases and distributed data access
- 20 with the following functionality:

- Replication and Synchronization;
- Partitioning of Data Files;
- Concurrency Controls;
- Transactional Capability; and
- 25 • Shared common Schemas.

Figure **28** shows logical system components and high-level information flows. None of the components depicted is physical. Multiple instances of each occur in the architecture.

- 30 The elements in Figure **28** are:

-85-

- NETWK **2224** - external access to the ISP **2100** from the network side;
- SVC I/F **2226** -the network interface into ISP;
- SYSTMS **2228** - external application such as Order Entry;
- G/W **2230** - a gateway to the ISP **2100** for external applications;
- 5 • dbAppl **2232** - a role requiring data access or update capabilities;
- dbClient **2234**- the primary role of the satellite domain;
- dbServer **2236**- the primary role of the central domain;
- dbAdmin **2238**- an administrative role for Data;
- dbMon **2240**- a monitoring role;
- 10 • I/F Admin **2242** administrative role for interfaces; and
- Ops **2244**- operations console.

d) Information Flow

The flows depicted in Figure **28** are logical abstractions; they are intended to
 15 characterize the type of information passing between the logical components.

The flows shown above are:

- Rest - data requests to the ISP from external systems;
- Resp -responses from the ISP to external requests;
- 20 • Access - data retrieval by applications within the ISP;
- Updates -data updates from applications within ISP;
- Evts, data related events sent to the monitor;
- Meas - data related metrics sent to the monitor;
- New Data -additions to ISP master data;
- 25 • Changed Data changes to ISP master data;
- Views - retrieving ISP master data;
- Subscriptions -asynchronous stream of ISP master data;
- Cache copies- a snapshot copy of ISP master data;
- Actions- any control activity; and
- 30 • Controls any control data.

-86-

e) Domain Associations

In general the Satellite domains **2222** of Data Management **2138** encompass:

- ISP Applications;
- 5 • External systems ;
- Network interfaces **2226** and system gateways **2230**; and
- Database client (dbClient) **2234**.

The Central domain for Data Management **2138** encompasses:

- 10 • Monitoring (dbMon) **2240**;
- Administration (dbAdmin) **2238**; and
- Database masters (dbServer) **2236**

4. Logical Description

- 15 The behavior of each Architecture component is described separately below:

a) Data Applications (dbAppl) 2232

This includes any ISP applications which require database access. Examples are the ISN NIDS servers, and the DAP Transaction Servers, The applications obtain their required data from the dbClient **2234** by attaching to the desired databases, and providing any required policy instructions. These applications also provide the database access on behalf of the external systems or network element such as Order Entry or Switch requested translations. Data applications support the following functionality:

- 25 • Updates: allow an application to insert, update, or delete data in an ISP database.
- Access requests allow an application to search for data, list multiple items, select items from a list or set, or iterate through members of a set.
- Events and Measurements are special forms of updates which are directed
- 30 to the monitoring function (dbMon) **2240**.

b) Data Management 2138**(1) Client Databases (dbClient) 2234**

5 The dbClients represent satellite copies of data. This is the only way for an application to access ISP data. Satellite copies of data need not match the format of data as stored on the dbServer **2236**.

The dbClients register with master databases (dbServer) **2236** for
10 Subscriptions or Cache Copies of data. Subscriptions are automatically maintained by dbServer **2236**, but Cache Copies must be refreshed when the version is out of date.

A critical aspect of dbClient **2234** is to ensure that data updates by
15 applications are serialized and synchronized with the master copies held by dbServer **2236**. However, it is just as reasonable for the dbClient to accept the update and only later synchronize the changes with the dbServer (at which time exception notifications could be conveyed back to the originating application). The choice to update in lock-step, or not, is a matter of
20 application policy not Data Management **2138**.

Only changes made to the dbServer master copies are forwarded to other dbClients.

25 If a dbClient **2234** becomes inactive or loses communications with the dbServer; it must resynchronize with the master. In severe cases, operator intervention may be required to reload an entire database or selected subsets.

30 The dbClient 2234 offers the following interface operations:

-88-

- Attach by an authorized application to a specified set of data;
 - Policy preferences to be set by an authorized application;
 - Select a specified view of the local copy of data;
 - Insert, Update, or Delete of the local copy of data;
 - 5 • Synchronize subscribed data with the dbServer; and
 - Expiration notifications from dbServer for cached data.
- Additionally, the dbClients submit Logs or Reports and signal problems to the monitor (dbMon) **2240**.

10 (2) Data Masters (dbServer) 2236

The dbServers **2236** play a central role in the protection of data. This is where data is 'owned' and master copies maintained. At least two copies of master data are maintained for reliability. Additional master copies may be deployed to improve data performance.

15 These copies are synchronized in lock-step. That is each update is required to obtain a corresponding master-lock in order to prevent update conflicts. The strict implementation policies may vary, but in general, all master copies must preserve serial ordering of updates, and provide the same view
20 of data and same integrity enforcement as any other master copy. The internal copies of data are transparent to the dbClients **2234**.

The dbServer **2236** includes the layers of business rules which describe or enforce the relationships between data items and which constrain particular
25 data values or formats. Every data update must pass these rules or is rejected. In this way dbServer ensures all data is managed as a single copy and all business rules are collected and applied uniformly.

The dbServer **2236** tracks when, and what kind of, data changes are made,
30 and provides logs and summary statistics to the monitor (dbMon) **2240**. Additionally these changes are forwarded to any active subscriptions and

-89-

Cache-copies are marked out of date via expiration messages.

The dbServer also provides security checks and authorizations, and ensures that selected items are encrypted before storage.

- 5 The dbServer supports the following interface operations:
- View selected data from dbServer;
 - Subscribe to selected data from dbServer;
 - Copy selected data into a cache-copy at a dbClient **2234**;
 - Refresh a dbClient cache with the current copy on demand;
 - 10 • New data insertion across all dbServer copies of the master;
 - Change data attributes across all dbServer copies; and
 - Cancel previous subscriptions and drop cache-copies of data.

(3) Data Administration (dbAdmin) 2238

- 15 Data Administration (dbAdmin) **2238** involves setting data policy, managing the logical and physical aspect of the databases, and securing and configuring the functional components of the Data Management **2138** domain. Data Management policies include security, distribution, integrity rules, performance requirements, and control of replications and partitions.
- 20 dbAdmin **2238** includes the physical control of data resources such as establishing data locations, allocating physical storage, allocating memory, loading data stores, optimizing access paths, and fixing database problems. dbAdmin 2238 also provides for logical control of data such as auditing, reconciling, migrating, cataloguing, and converting data.

25

The dbAdmin **2238** supports the following interface operations:

- Define the characteristics of a data type;
- Create logical containers of given dimensions;
- Relate two or more containers through an association;
- 30 • Constrain data values or relations through conditional triggers and actions;
- Place physical container for data in a given location;

-90-

- Move physical containers for data to new locations;
- Remove physical containers and their data;
- Load data from one container to another;
- Clear the data contents of a container; and
- 5 • Verify or reconcile the data contents of a container.

(4) Data Monitoring (dbMon) **2240**

The dbMon **2240** represents a monitoring function which captures all data-related events and statistical measurements from the ISP boundary gateways, dbClients **2234** and dbServers **2236**. The dbMon **2240** mechanisms are used to create audit trails and logs.

The dbMon typically presents a passive interface; data is fed to it. However monitoring is a hierarchical activity and further analysis and roll-up (compilation of data collected at intervals, such as every minute, into longer time segments, such as hours or days) occurs within dbMon. Additionally dbMon will send alerts when certain thresholds or conditions are met.

20 The rate and count of various metrics are used for evaluating quality of Service (QOS) , data performance, and other service level agreements. All exceptions and date errors are logged and flow to the dbMon for inspection, storage, and roll-up.

dbMon **2240** supports the following interface operations:

- Setting monitor controls, filters, and thresholds;
- Logging of data related activity;
- Reports of status, metrics, or audit results; and
- Signaling alarms, or alerts.

30	(5)	Data Management operations (Ops)	2244
----	-----	----------------------------------	------

-91-

The Operations consoles (Ops) **2244** provide the workstation-interface for the personnel monitoring, administering, and otherwise managing the system. The Ops consoles provide access to the operations interfaces for dbMon **2240**, dbAdmin **2238**, and dbServer **2236** described above. The Ops
 5 consoles **2244** also support the display of dynamic status through icon based maps of the various systems, interfaces, and applications within the Data management domain **2138**.

5. Physical Description

- 10 This section describes the Data Management **2138** physical architecture. It describes how a set of components could be deployed. A generalized deployment view is shown in Figure **29**. In Figure **29**:
- circles are used to represent physical sites,
 - boxes or combined boxes are computer nodes, and
 - 15 • functional roles are indicated by abbreviations.

The abbreviations used in Figure **29** are:

- OE - order entry systems **2250**;
- GW - ISP gateway **2230**;
- 20 • APP - application (dbAppl) **2232**;
- CL- a dbClient **2234**;
- SVR- a dbServer **2236**;
- ADM- a dbAdmin component **2238**;
- MON- a dbMon component **2240**; and
- 25 • Ops - operations console.

The functional roles of these elements were described above (see Logical Description of the Target Architecture) in connection with Figure **28**.

- 30 Each of the sites shown in Figure **29** is typically linked with one or more of the other sites by wide area network (WAN) links. The exact network configuration and sizing is left to a detailed engineering design task. It is

-92-

not common for a database copy to be distributed to the Order Entry (OE) sites **2251**, however in this architecture, entry sites are considered equivalent to satellite sites and will contain the dbClient functionality.

- 5 On the network-side of the ISP **2100**, Satellite sites **2252** each contain the dbClient **2234** too. These sites typically operate local area networks (LANs). The dbClients act as local repositories for network or system applications such as the ISN operator consoles, ARUs, or NCS switch requested translations.

10

The Central sites **2254** provide redundant data storage and data access paths to the dbClients **2234**. Central sites **2254** also provide roll-up monitoring (dbMon) functions although dbMon components **2240** could be deployed at satellite sites **2252** for increased performance.

15

The administrative functions are located at any desired operations or administration site **2254** but not necessarily in the same location as the dbMon. Administrative functions require the dbAdmin **2238**, plus an operations console **2244** for command and control. Remote operations sites

20 are able to access the dbAdmin nodes **2238** from wide-area or local-area connections. Each of the sites is backed-up by duplicate functional components at other sites and are connected by diverse, redundant links.

6. Technology Selection

- 25 The following section describes the various technology options which should be considered. The Data Management **2138** architecture does not require any particular technology to operate; however different technology choices will impact the resulting performance of the system.
- 30 Figure **30** depicts a set of technologies which are able to provide a very-high performance environment. Specific application requirements will determine

-93-

the minimum level of acceptable performance. Three general environments are shown.

- 5 • In the upper part, a multi-protocol routed network **2260** connects external and remote elements with the central data sites. Administrative terminals, and smaller mid-range computers are shown, plus a high-availability application platform such as Order Entry.
- 10 • In the center are large-scale high-performance machines **2262** with large data-storage devices; these would be typical of master databases and data processing, and data capture/tracking functions such as dbServer **2236** and dbMon **2240**.
- 15 • In the lower part of the diagram are local area processing and network interfaces **2264**, such as the ISN operator centers or DAP sites.

7. Implementations

- While much is known of the current ISP data systems, additional detailed requirements are necessary before any final implementations are decided.
- 20 These requirements must encompass existing ISN, NCS, EVS, NIA, and TMN system needs, plus all of the new products envisioned for Broadband, Internet, and Switchless applications.

8. Security

- 25 ISP data is a protected corporate resource. Data access is restricted and authenticated. Data related activity is tracked and audited. Data encryption is required for all stored passwords, PINS (personal identification numbers), private personnel records, and selected financial, business, and customer information. Secured data must not be transmitted in clear-text
- 30 forms.

9. Meta-Data

Meta-data is a form of data which comprises the rules for data driven logic.

Meta-data is used to describe and manage (i.e. manipulate) operational

5 forms of data. Under this architecture, as much control as possible is intended to be driven by meta-data. Meta-data (or data-driven logic) generally provides the most flexible run-time options. Meta-data is typically under the control of the system administrators.

10. Standard Database Technologies

Implementation of the proposed Data Management Architecture should take advantage of commercially available products whenever possible. Vendors offer database technology, replication services, Rules systems, Monitoring facilities, Console environments, and many other attractive offerings.

15

J. ISP Resource Management Model

This section describes the Resource Management **2150** Model as it relates to the ISP **2100** Architecture.

20 a) Scope

The Resource Management Model covers the cycle of resource allocation and de-allocation in terms of the relationships between a process that needs a resource, and the resource itself. This cycle starts with Resource

Registration and De-registration and continues to Resource Requisition,

25 Resource Acquisition, Resource Interaction and Resource Release.

b) Purpose

The Resource Management **2150** Model is meant to define common

architectural guidelines for the ISP development community in general, and for the ISP Architecture in particular.

c) Objectives

- 5 In the existing traditional ISP architecture, services control and manage their own physical and logical resources. Migration to an architecture that abstracts resources from services requires defining a management functionality that governs the relationships and interactions between resources and services. This functionality is represented by the Resource Management **2150** Model.

The objectives of the Resource Management Model are designed to allow for network-wide resource management and to optimize resource utilization, to enable resource sharing across the network:

- Abstract resources from services;
- 15 • Provide real-time access to resource status;
- Simplify the process of adding and removing resources;
- Provide secure and simple resource access; and
- Provide fair resource acquisition, so that no one user of resources may monopolize the use of resources.

20

d) Background Concepts

Generally, the Resource Management **2150** Model governs the relationships and interactions between the resources and the processes that utilize them.

- Before the model is presented, a solid understanding of the basic terminology and concepts used to explain the model should be established.
- 25 The following list presents these terms and concepts:

(1) Definitions

- Resource: A basic unit of work that provides a specific and well-

-96-

defined capability when invoked by an external process. Resources can be classified as logical, like a service engine and a speech recognition algorithm, or physical, like CPU, Memory and Switch ports. A resource may be Shared like an ATM link bandwidth or Disk space, or Dedicated like a VRU or a Switch port.

- Resource Pool: A set of registered resource members that share common capabilities.
- Service: A logical description of all activities and the interaction flow between the user of the network resources and the resources themselves.
- Policy: A set of rules that governs the actions taken on resource allocation and de-allocation, resource pool size thresholds and resource utilization thresholds.

(2) Concepts

- The Resource Management Model is a mechanism which governs and allows a set of functions to request, acquire and release resources to/from a resource pool through well-defined procedures and policies. The resource allocation and de-allocation process involves three phases:
 - Resource Requisition is the phase in which a process requests a resource from the Resource Manager **2150**.
 - Resource Acquisition: If the requested resource is available and the requesting process has the privilege to request it, the Resource Manager **2150** will grant the resource and the process can utilize it. Otherwise, the process has the choice to either abandon the resource allocation process and may try again later, or it may request that the Resource Manager **2150** grant it the resource whenever it becomes available or within a specified period.

-97-

- Resource Release: The allocated resource should be put back into the resource pool once the process no longer needs it. Based on the resource type, the process either releases the resource and the resource informs the Resource Manager of its new status, or the process itself informs the Resource Manager that the resource is available. In either case, the Resource Manager will restore the resource to the resource pool.

The Resource Management Model allows for the creation of resource pools and the specification of the policies governing them. The Resource Management Model allows resources to register and de-register as legitimate members of resource pools.

Resource Management Model policies enforce load balancing, failover and least cost algorithms and prevent services from monopolizing resources. The Resource Management Model tracks resource utilization and automatically takes corrective action when resource pools are not sufficient to meet demand. Any service should be able to access and utilize any available resource across the network as long as it has the privilege to do so.

The Resource Management Model adopted the OSI Object Oriented approach for modeling resources. Under this model, each resource is represented by a Managed Object (MO). Each MO is defined in terms of the following aspects:

- Attributes: The attributes of a MO represent its properties and are used to describe its characteristics and current states. Each attribute is associated with a value, for example the value CURRENT_STATE attribute of a MO could be IDLE.
- Operations: Each MO has a set of operations that are allowed to be performed on it. These operations are:
 - Create: to create a new MO
 - Delete: to delete an existing MO
 - Action: to perform a specific operation such as SHUTDOWN.

-98-

- Get Value: to obtain a specific MO attribute value
- Add Value: to add specific MO attribute value
- Remove Value: to delete a specific MO attribute value from a set of values.
- 5 • Replace Value: to replace an existing MO attribute value(s) with a new one.
- Set Value: to set a specific MO attribute to its default value.
- Notification: Each MO can report or notify its status to the management entity. This could be viewed as triggers or traps.
- 10 • Behavior: The behavior of an MO is represented by how it reacts to a specific operation and the constraints imposed on this reaction. The MO may react to either external stimuli or internal stimuli. An external stimuli is represented by a message that carries an operation. The internal stimuli, however, is an internal event that occurred to
- 15 the MO like the expiration of a timer. A constraint on how the MO should react to the expired timer may be imposed by specifying how many times the timers has to expire before the MO can report it.

All elements that need to utilize, manipulate or monitor a resource need to
20 treat it as a MO and need to access it through the operations defined above.
Concerned elements that need to know the status of a resource need to
know how to receive and react to events generated by that resource.

Global and Local Resource Management:

25

The Resource Management Model is hierarchical with at least two levels of management: Local Resource Manager (LRM) **2190** and Global Resource Manager (GRM) **2188**. Each RM, Local and Global, has its own domain and functionality.

30

-99-

2. The Local Resource Manager (LRM):

- Domain: The domain of the LRM is restricted to a specific resource pool (RP) that belongs to a specific locale of the network. Multiple LRMs could exist in a single locale, each LRM may be responsible for managing a specific resource pool.
- Function: The main functionality of the LRM is to facilitate the resource allocation and de-allocation process between a process and a resource according the Resource Management Model guidelines.

3. The Global Resource Manager (GRM) 2188:

- Domain: The domain of the GRM **2188** covers all registered resources in all resource pools across the network.
- Function: The main function of the GRM is to help the LRM **2190** locate a resource that is not available in the LRM domain.

Figure **31** illustrates the domains of the GRM **2188** and LRM **2190** within network **2270**.

4. The Resource Management Model (RMM)

The Resource Management Model is based on the concept of Dynamic Resource Allocation as opposed to Static Configuration. The Dynamic Resource Allocation concept implies that there is no pre-defined static relationship between resources and the processes utilizing them. The allocation and de-allocation process is based on supply and demand. The Resource Managers **2150** will be aware of the existence of the resources and the processes needing resources can acquire them through the Resource Managers **2150**. On the other hand, Static Configuration implies a pre-defined relationship between each resource and the process that needs it.

-100-

In such a case, there is no need for a management entity to manage these resources. The process dealing with the resources can achieve that directly. Dynamic Resource Allocation and Static Configuration represent the two extremes of the resource management paradigms. Paradigms that fall
5 between these extremes may exist.

The Resource Management Model describes the behavior of the LRM **2190** and GRM **2188** and the logical relationships and interactions between them. It also describes the rules and policies that govern the resource allocation
10 and de-allocation process between the LRM/GRM and the processes needing the resources.

a) Simple Resource Management Model

Realizing that resource allocation and de-allocation could involve a complex
15 process, a simple form of this process is presented here as an introduction to the actual model. Simple resource allocation and de-allocation is achieved through six steps. Figure **32** depicts these steps.

1. A process **2271** requests the resource **2173** from the resource manager **2150**.
- 20 2. The resource manager **2150** allocates the resource **2173**.
3. The resource manager **2150** grants the allocated resource **2173** to the requesting process **2271**.
4. The process **2271** interacts with the resource **2273**.
5. When the process **2271** is finished with the resource **2273**, it
25 informs the resource.
6. The resource **2273** releases itself back to the resource manager **2150**.

-101-

b) The Resource Management Model Logical Elements:

The Resource Management Model is represented by a set of logical elements that interact and co-operate with each other in order to achieve the objectives mentioned earlier. These elements are shown in Figure **33** and include: Resource Pool (RP) **2272**, LRM **2190**, GRM **2188** and Resource Management Information Base (RMIB) **2274**.

(1) Resource Pool (RP) 2272

- 10 All resources that are of the same type, share common attributes or provide the same capabilities, and are located in the same network locale may be logically grouped together to form a Resource Pool (RP) **2272**. Each RP will have its own LRM **2190**.

15 (2) The Local Resource Manager (LRM) 2190

The LRM **2190** is the element that is responsible for the management of a specific RP **2272**. All processes that need to utilize a resource from a RP that is managed by a LRM should gain access to the resource through that LRM and by using the simple Resource Management Model described above.

20

(3) The Global Resource Manager (GRM) 2188

The GRM **2188** is the entity that has a global view of the resource pools across the network. The GRM gains this global view through the LRMs **2190**. All LRMs update the GRM with RP **2272** status and statistics. There are cases where a certain LRM can not allocate a resource because all local resources are busy or because the requested resource belongs to another locale. In such cases, the LRM can consult with the GRM to locate the requested resource across the network.

25

-102-

(4) The Resource Management Information Base
(RMIB) 2274

As mentioned above, all resources will be treated as managed objects (MO). The RMIB **2274** is the database that contains all the information about all MOs across the network. MO information includes object definition, status, operation, etc. The RMIB is part of the ISP Data Management Model. All LRMs and the GRM can access the RMIB and can have their own view and access privileges of the MO's information through the ISP Data Management Model.

10

5. Component Interactions

To perform their tasks, the Resource Management Model elements must interact and co-operate within the rules, policies and guidelines of the Resource Management Model. The following sections explain how these entities interact with each other.

15

a) Entity Relationship (ER) Diagram (Figure 33):

In Figure **33**, each rectangle represents one entity, the verb between the "<>" implies the relationship between two entities and the square brackets "[]" imply that the direction of the relationship goes from the bracketed number to the non bracketed one. The numbers imply is the relationship is 1-to-1, 1-to-many or many-to-many.

20

Figure **33** can be read as follows:

1. One LRM **2190** manages one RP **2272**.
2. Many LRMs **2190** access the RMIB **2274**.
3. Many LRMs **2190** access the GRMs **2188**.
4. Many GRMs **2188** access the RMIB **2274**.

25

b) Registration and De-registration

Resource registration and de-registration applies only on the set of resources that have to be dynamically managed. There are some cases where resources are statically assigned.

5

LRMs **2190** operate on resource pools **2272** where each resource pool contains a set of resource members. In order for the LRM to manage a certain resource, the resource has to inform the LRM of its existence and status. Also, the GRM **2188** needs to be aware of the availability of the resources across the network in order to be able to locate a certain resource.

10

The following registration and de-registration guidelines should be applied on all resources that are to be dynamically managed:

- All resources must register to their LRM **2190** as members of a specific resource pool **2272**.
- All resources must de-register from their LRM **2190** if, for any reason, they need to shutdown or be taken out of service.
- All resources must report their availability status to their LRM **2190**.
- All LRMs must update the GRM **2188** with the latest resource availability based on the registered and de-registered resources.

15

20

c) GRM, LRM and RP Interactions

Every RP **2272** will be managed by an LRM **2190**. Each process that needs a specific resource type will be assigned an LRM that will facilitate the resource access. When the process needs a resource it must request it through its assigned LRM. When the LRM receives a request for a resource, two cases may occur:

25

1. Resource is available: In this case, the LRM allocates a resource member of the pool and passes a resource handle to the process. The process interacts with the resource until it is done with it. Based on the resource type, once the process is done with the resource, it either informs

30

-104-

the resource that it is done with it, and the resource itself informs its LRM that it is available, or it releases the resource and informs the LRM that it is no longer using the resource.

2. Resource is not available: In this case, the LRM **2190** consults with the GRM **2188** for an external resource pool that contains the requested resource. If no external resource is available, the LRM informs the requesting process that no resources are available. In this case, the requesting process may:

- give up and try again,

- request that the LRM allocate the resource whenever it becomes available, or

- request that the LRM allocates the resource if it becomes available within a specified period of time.

If an external resource is available, the GRM **2188** passes location and access information to the LRM **2190**. Then the LRM either:

- allocates the resource on the behalf of the requesting process and passes a resource handle to it (In this case the resource allocation through the GRM is transparent to the process), or

- advises the requesting process to contact the LRM that manages the located resource.

d) GRM, LRM and RMIB Interactions

The RMIB **2274** contains all information and status of all managed resources across the network. Each LRM **2190** will have a view of the RMIB **2274** that maps to the RP **2272** it manages. The GRM **2188**, on the other hand, has a total view of all resources across the network. This view consists of all LRMs views. The GRM's total view enables it to locate resources across the network.

In order for the RMIB **2274** to keep accurate resource information, each

-105-

LRM **2190** must update the RMIB with the latest resource status. This includes adding resources, removing resources and updating resource states.

- 5 Both the LRM **2190** and GRM **2188** can gain their access and view of the RMIB **2274** through the ISP Data Management entity. The actual management of the RMIB data belongs to the ISP Data Management entity. The LRM and GRM are only responsible for updating the RMIB.

10 **K. Operational Support Model**

1. Introduction

Most of the existing ISP service platforms were developed independently, each with it's own set of Operational Support features. The amount of time required to learn how to operate a given set of platforms increases with the
15 number of platforms. The ISP service platforms need to migrate to an architecture with a common model for all of its Operational Support features across all of its products. This requires defining a model that will support current needs and will withstand or bend to the changes that will occur in the future. The Operational Support Model (OSM) defines a
20 framework for implementation of management support for the ISP **2100**.

a) Purpose

The purpose of the Operational Support Model is to:

- achieve operational simplicity by integrating the management platform for
25 ISP resources;
- reduce the learning curve for operational personnel by providing a common management infrastructure;
- reduce the cost of management systems by reducing overlapping management system development;

-106-

- improve time to market for ISP services by providing a common management infrastructure for all of the ISP services and network elements; and

- provide a framework for managing ISP physical resources (hardware) and
- 5 logical resources (software).

b) Scope

The OSM described here provides for the distributed management of ISP physical network elements and the services that run on them. The

10 management framework described herein could also be extended to the management of logical (software) resources. However, the architecture presented here will help map utilization and faults on physical resources to their resulting impact on services.

The management services occur within four layers

- 15
- Planning,
 - Service Management,
 - Network Layers, and
 - Network Elements.

Information within the layers falls into four functional areas:

- 20
- Configuration Management,
 - Fault Management,
 - Resource Measurement, and
 - Accounting.

25 The use of a common Operational Support Model for all of the ISP will enhance the operation of the ISP, and simplify the designs of future products and services within the ISP. This operational support architecture is consistent with the ITU Telecommunications Management Network (TMN) standards.

c) Definitions

Managed Object: A resource that is monitored, and controlled by one or more management systems. Managed objects are located within managed systems and may be embedded in other managed objects. A managed object
5 may be a logical or physical resource, and a resource may be represented by more than one managed object (more than one view of the object).

Managed System: One or more managed objects.

Management Sub-Domain: A Management domain that is wholly located within a parent management domain.

10 Management System: An application process within a managed domain which effects monitoring and control functions on managed objects and/or management sub-domains.

Management Information Base : A MIB contains information about managed objects.

15 Management Domain: A collection of one or more management systems, and zero or more managed systems and management sub-domains.

Network Element: The Telecommunications network consist of many types of analog and digital telecommunications equipment and associated support equipment, such as transmission systems, switching systems, multiplexes,
20 signaling terminals, front-end processors, mainframes, cluster controllers, file servers, LANs, WANs, Routers, Bridges, Gateways, Ethernet Switches, Hubs, X.25 links, SS7 links, etc. When managed, such equipment is generally referred to as a network element (NE).

Domain: The management environment may be partitioned in a number of ways such as functionally (fault, service....), geographical, organizational structure, etc.
25

Operations Systems: The management functions are resident in the Operations System.

30 2. The Operational Support Model

Figure 34 shows the four management layers **2300**, **2302**, **2304** and **2306**

-108-

of the Operational Support Model **2308** over the network elements **2310**. The Operational Support Model **2308** supports the day to day management of the ISP **2100**. The model is organized along three dimensions. Those dimensions are the layers **2300-2306**, the functional area within those layers, and the activities that provide the management services. Managed objects (a resource) are monitored, controlled, and altered by the management system.

a) The Functional Model

- 10 The following sections describe the functional areas as they occur within the management layers **2300-2306**.

(1) Planning

- 15 The ISP Planning Layer **2300** is the repository for data collected about the ISP **2100**, and the place where that data is to provide additional value.

- Configuration Management **2312**: Setting of policy, and goals.
- Fault Management **2314**: Predicting of mean time to failure.
- Resource Measurement **2316**: Predicting future resource needs (trending, capacity, service agreement compliance, maintenance agreement, work force).
- Accounting: Determine cost of providing services in order to support service pricing decisions.

(2) Service Management

- 25 The Service Ordering, Deployment, Provisioning, Quality of Service agreements, and Quality of service monitoring are in the ISP Service Management layer **2302**. Customers will have a restricted view of the SM layer **2302** to monitor and control their services. The SM layer provides a manager(s) that interacts with the agents in the NLMs. The SM layer also

-109-

provides an agent(s) that interacts with the manager(s) in the Planning layer
2300. Managers within the SM layer may also interact with other managers in the SM layer. In that case there are manager-agent relationships at the peer level.

- 5 • Configuration Management **2320**: Service Definition, Service Activation, Customer Definition, Customer Activation, Service Characteristics, Customer Characteristics, hardware provisioning, software provisioning, provisioning of other data or other resources.
- Fault Management **2322**: Monitor and report violations of service
- 10 agreement. Testing.
- Resource Measurement **2324**: Predict the violation of a service agreement and flag potential resource shortages. Predict the needs of current and future (trending) services.
- Accounting **2326**: Process and forward Accounting information.

15

-110-

Network Layer Management:

The ISP Network Layer Management (NLM) Layer **2304** has the responsibility for the management of all the network elements, as presented by the Element Management, both individually and as a set. It is not concerned with how a particular element provides services internally. The NLM layer **2304** provides a manager(s) that interacts with the agents in the EMs **2306**. The NLM layer also provides an agent(s) that interacts with the manager(s) in the SM layer **2302**. Managers within the NLM layer **2304** may also interact other managers in the NLM layer. In that case there are manager agent relationships at the peer level.

- Configuration Management **2328** provides functions to define the characteristics of the local and remote resources and services from a network wide perspective.
- Fault Management **2330** provides functions to detect, report, isolate, and correct faults that occur across multiple NEs.
- Resource Measurement **2332** provides for the network wide measurement, analysis, and reporting of resource utilization from a capacity perspective.
- Accounting **2334** consolidates Accounting information from multiple sources.

(3) Element Management

The Element Management Layer **2306** is responsible for the NEs **2310** on an individual basis and supports an abstraction of the functions provided by the NEs. The EM layer **2306** provides a manager(s) that interact with the agents in the NEs. The EM layer also provides an agent(s) that interact with the manager(s) in the NLM layer **2304**. Managers within the EM layer **2306** may also interact other managers in the EM layer. In that case there are manager agent relationships at the peer level.

- Configuration Management **2336** provides functions to define the characteristics of the local and remote resources and services.

-111-

- Fault Management **2338** provides functions to detect, report, isolate, and correct faults.
- Resource Measurement **2340** provides for the measurement, analysis, and reporting of resource utilization from a capacity perspective.
- 5 • Accounting **2342** provides for the measurement and reporting of resource utilization from an accounting perspective.

b) Network Element

10 The computers, processes, switches, VRUs, internet gateways, and other equipment that provide the network capabilities are Network Elements **2310**. NEs provide agents to perform operations on the behalf of the Element Management Layer **2306**.

c) Information Model

15 Figure **35** shows manager agent interaction. Telecommunications network management is a distributed information application process. It involves the interchange of management information between a distributed set of management application processes for the purpose of monitoring and controlling the network resources (NE) **2310**. For the purpose of this
20 exchange of information the management processes take on the role of either manager **2350** or agent **2352**. The manager **2350** role is to direct management operation requests to the agent **2352**, receive the results of an operation, receive event notification, and process the received information. The role of the agent **2352** is to respond to the manager's request by
25 performing the appropriate operation on the managed objects **2354**, and directing any responses or notifications to the manager. One manager **2350** may interact with many agents **2352**, and the agent may interact with more than one manager. Managers may be cascaded in that a higher level manager acts on managed objects through a lower level manager. In that
30 case the lower level manager acts in both manager and agent roles.

3. The Protocol Model

a) Protocols

The exchange of information between manager and agent relies on a set of communications protocols. TMN, which offers a good model, uses the Common Management Information Services (CMIS) and Common Management Information Protocol (CMIP) as defined in Recommendations X.710, and X.711. This provides a peer-to-peer communications protocol based on ITU's Application Common Service Element (X.217 service description & X.227 protocol description) and Remote Operation Service Element (X.219 service description & X.229 protocol description). FTAM is also supported as an upper layer protocol for file transfers. The use of these upper layer protocols is described in Recommendation X.812. The transport protocols are described in Recommendation X.811. Recommendation X.811 also describes the interworking between different lower layer protocols. This set of protocols is referred to as Q3.

b) Common context

In order to share information between processes there needs to be a common understanding of the interpretation of the information exchanged. ASN.1 (X.209) with BER could be used to develop this common understanding for all PDU exchanged between the management processes (manager/agent).

c) Services of the upper layer

The following identifies the minimum services required of the service layer and is modeled after the TMN CMIS services.

SET: To add, remove, or replace the value of an

-113-

attribute.

GET: To read the value of an attribute.

CANCEL-GET: To cancel a previously issued GET.

ACTION: To request an object to perform a certain action.

5 CREATE: To create an object.

DELETE: To remove an object.

EVENT-REPORT: Allows the network resource to announce an event.

4. The Physical Model

10 Figure **36** shows the ISP **2100** physical model.

5. Interface Points

Mediation Device **2360** provides conversion from one information model to the ISP information model. Gateways **2362** are used to connect to

15 management systems outside of the ISP. These gateways will provide the necessary functions for operation with both ISP compliant systems, and non-compliant systems. The gateways may contain mediation devices **2360**.

Figure **36** identifies nine interface points. The protocols associated with those interface points are:

20

1. There are two upper layer protocols. The protocol for communications with the workstation and the ISP upper layer for all other operational support communications. The lower layer is TCP/IP over Ethernet.

25 2. The upper layer is the protocol for communications with workstation **2364**, and the lower layer is TCP/IP over Ethernet.

3,4. The upper layer is the ISP upper layer, and the lower layer is TCP/IP over Ethernet.

30

-114-

5. The proprietary protocols are the of legacy systems that are not compatible with the supported interfaces. Equipment that provides a Simple Network Management Protocol (SNMP) interface will be supported with Mediation Devices.

5

6,7,8,9. Gateways by their nature will support ISP compliant and non-compliant interfaces. Gateways to enterprise internal systems could include such as the Order Entry system, or an enterprise wide TMN system.

10 **The ISP Realization of the Operational Support Model**

Figure **37** shows operational support realization.

6. General

15 The Operational Support Model provides a conceptual framework for building the Operational Support System. Figure **37** represents an ISP realization of this conceptual model. In this implementation of that model all the ISP Network Elements would be represented to the Operational Support System by a Management Information Base (MIB) **2370** and the
20 agent process that acts upon the objects in the MIB.

Field support personnel have two levels from which the ISP **2100** will be managed.

1. For trouble-shooting, the Network Layers Manager **2372** gives field
25 support a picture of the ISP as a whole. The process of detecting, isolating, and correcting problems begins from there. From that layer, problems could be isolated to a single Network Element. Individual Network Elements are accessible from the Network Element Managers **2374** and would allow a more detailed level of monitoring, control, configuration, and testing. The
30 centralized view of the ISP is missing from today's ISP, but many recognize its importance.

-115-

For configuration the Network Layers Manager **2370** provides an ISP-wide view, and interacts with the Network Element Managers **2374** to configure Network Elements in a consistent manner. This will help insure that the ISP configuration is consistent across all platforms. The ability to change a piece of information in one place and have it automatically distributed ISP-wide is a powerful tool that has not been possible with the current ISP management framework.

Once a service definition has been created from the Service Creation Environment **2376**, the Service Manager **2378** is used to place it in the ISP network, and provision the network for the new service. Customers for a service are provisioned through the Service Manager **2378**. As a part of provisioning customers the Service Manager predicts resource utilization, and determines if new resources need to be added to handle the customer's use of a service. It uses the current utilization statistics as a basis for that determination. Once a customer is activated, the Service Manager monitors the customer's usage of the service to determine if the quality of service agreement is being met. As customer utilization of the services increases the Service Manager **2378** predicts the need to add resources to the ISP network. This Service Management, with appropriate restrictions, can be extended to customers as another service. While Service Creation is the talk of the IN world, it needs a Service Manager that is integrated with the rest of the system, and that is one of the purposes of this model.

Finally, for planning personnel (non-field support), the Planning Manager **2380** analyzes the ISP-wide resource utilization to determine future needs, and to allocate cost to different services to determine the cost of a service as the basis for future service pricing.

-116-

L. Physical Network Model**1. Introduction**

This section describes the Physical Network aspects of the Intelligent Services Platform (ISP) **2100** Architecture.

5

a) Purpose

The Physical Network Model covers the:

- Logical Architecture Mapping;
- Information Flows; and
- 10 • Platform Deployment in the production environment of the architecture.

b) Scope

This model defines the terminology associated with the physical network, describes the interactions between various domains and provides examples
15 of realizations of the architecture.

c) Objectives

The objectives of this model are to:

- Create a model for identifying various network platforms;
- Classify Information Flow;
- 20 • Provide standard nomenclature;
- Provide rules for systems deployment; and
- Guide future technology selections.

2. Information Flow

25 One of the key aspects of the intelligent network (IN) is the Information Flow across various platforms installed in the network. By identifying types of information and classifying them, the network serves the needs of IN.

-117-

Customers interact with IN in a series of call flows. Calls may be audio-centric (as in the conventional ISP products), multimedia-based (as in internetMCI user using the web browser), video-based (as in video-on-demand) or a combination of contents.

Information can be classified as follows:

- Content;
- Signaling; or
- Data.

Normally, a customer interacting with the intelligent network will require all three types of information flows.

a) Content

Content flows contain the primary information being transported. Examples of this are analog voice, packet switched data, streamed video and leased line traffic. This is customer's property that IN must deliver with minimum loss, minimum latency and optimal cost. The IN elements are standardized such that the transport fabric supports more connectivity suites, in order to allow content to flow in the same channels with flow of other information.

b) Signaling

Signaling flows contain control information used by network elements. ISUP RLT/IMT, TCP/IP domain name lookups and ISDN Q.931 are all instances of this. The IN requires, uses and generates this information. Signaling information coordinates the various network platforms and allows intelligent call flow across the network. In fact, in a SCE-based IN, service deployment will also require signaling information flowing across the fabric.

-118-

c) Data

Data flows contain information produced by a call flow, including crucial billing data records often produced by the fabric and certain network platforms.

5

3. Terminology

Network: A set of interconnected network elements capable of transporting content, signaling and/or data. MCI's IXC switch fabric, the ISP extended WAN, and the Internet backbone are classic examples of networks. Current
10 installations tend to carry different contents on different networks, each of which is specialized for specific content transmission. Both technology and customer requirements (for on-demand high bandwidth) will require carriers to use more unified networks for the majority of the traffic. This will require the fabric to allow for different content characteristics and protocols along
15 the same channels. Another aspect of this will be more uniform content-independent signaling.

Site: A set of physical entities collocated in a geographically local area. In the current ISP architecture, instances of sites are Operator Center, ISNAP Site (which also has ARU's) and an EVS site. By the very definition, the NT
20 and DSC switches are NOT part of the site. They are instead part of the Transport Network (see below). In the architecture, a group of (geographically collocated) Service Engines (SE), Special Resources (SR), Data Servers (DS) along with Network Interfaces and Links form a site.

Network Element: A physical entity connecting to the Transport Networks
25 through Network Interfaces. Examples of this are ACP, EVS SIP, MTOC, Videoconference Reservation Server, DAP Transaction Server, and NAS. In the next few years, elements such as web servers, voice authentication servers, video streamers and network call record stores will join the present family of network elements.

30 **Network Interface:** Equipment enabling connectivity of Network Elements to the Transport Networks. DS1 CSU/DSU, 10BaseT Ethernet interface card

-119-

and ACD ports are network interfaces. With the architecture of the preferred embodiment, network interfaces will provide a well-understood uniform set of API's for communication.

Link: Connection between 2 or more Network Interfaces which are at different sites. A link may be a segment of OC-12 SONET Fiber or 100mbps dual ring FDDI section. In the coming years, IN must handle network links such as ISO Ethernet WAN hub links and gigabit rate OC-48's.

Connection: an attachment of two or more Network Interfaces which are at the same site.

Figure **38** shows a representation of a physical network **2400** schematic. Networks **2401** contain network elements **2402** at sites **2404** are interconnected through network interfaces **2406** and one or more gateways **2408**.

4. Entity Relationships

Entity relationships as shown in Figure **39** have been arrived at as part of the physical network modeling rules. Some of these rules allow for generalities that future demands and some will constrain definitions to avoid conflicts.

1. A Network **2401** spans one or more sites **2404**, and contains one or more network elements **2402**.
2. A Site **2404** contains one or more network elements **2402**.
3. A Network Element **2402** is located in only one Site **2404**.
4. A Link **2420** connects two or more Sites **2404**.
5. A Connection **2422** connects two or more Network Elements.
6. A Network Element **2402** contains one or more Network Interfaces **2406**.

The preferred embodiment integrates product and service offerings for MCI's business customers. The initial embodiment focuses on a limited product

-120-

set. Requirements for an interface have been identified to capitalize on the integration of these services. The interface provides user-manageability of features, distribution list capabilities, and a centralized message database.

5 **VIII. INTELLIGENT NETWORK**

All of the platform's support services have been consolidated onto one platform. The consolidation of platforms enables shared feature/functionality of services to create a common look and feel of features.

10

A. Network Management

The architecture is designed such that it can be remotely monitored by an MCI operations support group. This remote monitoring capability provides MCI the ability to:

15

- Identify degraded or broken connectivity between:
 - platforms, servers or nodes that must pass information (i.e., objects) to the "universal inbox",
 - platforms, servers or nodes responsible for retrieving messages and

20

- delivering messages,
 - the "universal inbox" and the PC Client messaging interface,
 - the "universal inbox" and the Message Center interface,
 - platforms, servers or nodes that must pass profile information to Profile, and

25

- platforms, servers or nodes that must pass profile information to the ARU;

- Identify degraded application processes and isolate the process that is degraded;
- Identify hardware failure; and
- Generate alarms that can be detected and received by an internal MCI

30

monitoring group for all application process, hardware or interface

-121-

failures.

In addition, remote access to system architecture components is provided to the remote monitoring and support group such that they can perform
5 remote diagnostics to isolate the cause of the problem.

B. Customer Service

Customer Service teams support all services. Customer support is provided to customers in a seamless manner and encompasses the complete product
10 life cycle including:

- Alpha tests;
- Beta tests;
- Commercial release; and
- Identification of enhancements to address customer feedback or
15 additional customer support requirements

Comprehensive and coordinated support procedures ensure complete customer support from inception to termination. Customer service is provided from the time the Account Team submits the order until the customer cancels the account. Comprehensive and coordinated customer
20 support entails the following:

- A one-stop, direct access, customer service group to support ARU or VRU problems, WWW Browser problems or PC Client problems.
- A staff that is well trained on diagnosing problems associated with access (ARU, WWW Browser or PC Client), the user interface (ARU, WWW
25 Browser or PC Client), the application (Message Center or Profile Management) or the back-end system interfaces (universal inbox, directlineMCI voicemail/faxmail platform, Fax Broadcast System, SkyTel Paging server, order entry systems, billing systems, etc.)
- A staff that has on-line access to databases with information about
30 ARU or VRU capabilities, WWW Browser capabilities, identified hardware issues and identified application issues

-122-

- 7 x 24 customer support
- a single toll free number (800 or 888) with direct access to the customer service group
- seamless first, second and third level support for most troubles where:

5 - Level 1 support is the first support representative answering the telephone. They are expected to be able to resolve the most commonly asked questions or problems reported by customers. These questions or problems typically deal with access type (ARU, WWW Browser, PC Client), dial-up communication for the WWW Browser or PC Client, installation or basic
10 computer (PC, workstation, terminal) hardware questions. Additionally they are able to open and update trouble tickets, and reactivate customers' passwords.

- Level 2 support is provided within the customer support group when referrals to more experienced technical experts is necessary.

15 - Level 3 support may involve an outside vendor for on-site hardware support for the customer or an internal MCI engineering or support group depending on the nature of the problem. The customer support group will be able to track the status of the customer visit and add the identified problem to both the customer support databases.

20

- Level 4 support will continue to be provided by the Systems Engineering programmers.

- Staffing levels to provide acceptable customer hold times and abandon rates.

25 • A staff that has on-line access to the order entry and billing systems.

- Automatically generate weekly reports that detail volume of calls made, received, average hold-time of calls and number of trouble tickets opened/closed/escalated.

30

C. Accounting

Accounting is supported according to current MCI procedures.

D. Commissions

Commissions are supported according to current MCI procedures.

5 E. Reporting

Reporting is required for revenue tracking, internal and external customer installation/sales, usage and product/service performance. Weekly and monthly fulfillment reports are required from the fulfillment house(s). These fulfillment reports correlate the number of orders received and number of orders delivered. In addition, reporting identifies the number of different subscribers accessing Profile Management or the Message Center through the WWW Site.

F. Security

15 Security is enforced in accordance with MCI's published policies and procedures for Internet security. In addition, security is designed into the WWW Browser and ARU interface options to verify and validate user access to directlineMCI profiles, Message Center, Personal Home Page calendars and Personal Home Page configurations.

20

G. Trouble Handling

Trouble reporting of problems is documented and tracked in a single database. All troubles are supported according to the Network Services Trouble Handling System (NSTHS) guidelines. Any Service Level Agreements (SLAs) defined between MCI organizations are structured to support NSTHS.

25

Any troubles that require a software fix are closed in the trouble reporting database and opened as a Problem Report (PR) in the Problem Tracking System. This Problem Tracking System is used during all test phases of and is accessible by all engineering and support organizations.

IX. ENHANCED PERSONAL SERVICES

Throughout this description, the following terms will be used:

5	Term	Represents
	Server	Both the hardware platform and a TCP service
	Web Server	AIX 4.2 system running Netscape Commerce Server
	HTTP Daemon	
	Welcome Server	
10	Application Server	
	The Web Servers running as Welcome Servers will be running the Netscape Commerce Server HTTP Daemon in secure as well as normal mode. The Web Servers operating as various application servers will run this daemon in secure mode only. The Secure Mode uses SSLv2.	

15 **A. Web Server Architecture**

The Web Servers are located in a DMZ. The DMZ houses the Web Servers and associated Database Clients as required. The database clients do not hold any data, but provide an interface to the data repositories behind the corporate firewall.

20 The Web space uses Round-Robin addressing for name resolution. The Domain name is registered with the administrators of mci.com domain, with a sub-netted (internally autonomous) address space allocated for galileo.mci.com domain.

25 Figure **40** shows the sequence of events leading to a successful login.

1. Welcome Server 450

This Web Server runs both the secure and normal HTTP daemons. The

-125-

primary function of this server is to authenticate user **452** at login time. The authentication requires the use of Java and a switch from normal to secure mode operation. There are one or more Welcome servers **450** in the DMZ. The information provided by the Welcome server **450** is stateless. The
5 statelessness means that there is no need to synchronize multiple Welcome Servers **450**.

The Welcome server's first task is to authenticate the user. This requires the use of single use TOKENS, Passcode authentication and Hostile IP filtering.
10 The first is done using a Token Server **454**, while the other two will be done using direct database **456** access.

In case of failed authentication, the user **452** is shown a screen that mentions all the reasons (except Hostile-IP) why the attempt may have
15 failed. This screen automatically leads the users back to the initial login screen.

Welcome server **450's** last task, after a successful authentication, is to send a service selection screen to the user **452**. The Service Selection screen
20 directs the user to an appropriate Application Server. The user selects the Application, but an HTML file in the Server Section page determines the Application Server. This allows the Welcome Servers **450** to do rudimentary load balancing.

25 All the Welcome Servers **450** in the DMZ are mapped to www.galileo.mci.com. The implementation of DNS also allows galileo.mci.com to map to www.galileo.mci.com.

2. Token Server 454

30 This is a database client and not a Web Server. The Token servers **454** are used by Welcome Servers **450** to issue a TOKEN to login attempts. The

-126-

issued TOKEN, once validated, is used to track the state information for a connection by the Application Servers. The TOKEN information is be maintained in a database on a database server **456** (repository) behind the corporate firewall.

5 The Token Servers **454** do the following tasks:

1. Issue single use TOKEN during authentication phase.
2. Validate single use TOKEN (mark it for multi use).
3. Validate multi-use TOKEN.
4. Re-validate multi-use TOKEN.

10

The Token Servers **454** are required to issue a unique TOKEN on every new request. This mandates a communication link between multiple Token Servers in order to avoid conflict of TOKEN values issued. This conflict is eliminated by assigning ranges to each Token Server **454**.

15

The TOKEN is a sixteen character quantity made up of 62 possible character values in the set [0-9A-Za-z]. The characters in positions 0,1 and 2 for each TOKEN issued by the Token Server are fixed. These character values are assigned to each Token Server at configuration time. The character at position 0 is used as physical location identifier. The character at position 1 identifies the server at the location while the character at position 2 remains fixed at '0'. This character could be used to identify the version number for the Token Server.

20

25 The remaining 13 characters of the TOKEN are generated sequentially using the same 62 character set described above. At startup the TOKEN servers assign the current system time to the character positions 15-10, and set positions 9-3 to '0'. The TOKEN values are then incremented sequentially on positions 15-3 with position 3 being least significant. The character encoding assumes the following order for high to low digit values : 'z'-'a', 'Z'-'A', '9'-'0'.

30

-127-

The above scheme generates unique tokens if the system time is computed in 4 byte values, which compute to 6 base-62 characters in positions 15-10. The other assumption is that the scheme does not generate more than 62^7 ($35 \cdot 10^{12}$) TOKENS in one second on any given Token Server in any
5 embodiment.

The use of TOKEN ranges allows the use of multiple Token Servers in the Domain without any need for explicit synchronization. The method accommodates a maximum 62 sites, each having no more than 62 Token
10 Servers. An alternate embodiment would accommodate more sites.

All of the Token Servers in the DMZ are mapped to token.galileo.mci.com. The initial embodiment contains two Token Servers **454**. These Token Servers **454** are physically identical to the Welcome Servers **450**, i.e., the
15 Token Service daemon will run on the same machine that also runs the HTTP daemon for the Welcome service. In another embodiment, the two run on different systems.

The Welcome Server(s) **450** use the Token Server(s) **454** to get a single use
20 TOKEN during the authentication phase of the connection. Once authenticated, the Welcome Server **450** marks the TOKEN valid and marks it for multiple use. This multi-use TOKEN accompanies the service selection screen sent to the user by the Welcome Server.

25 The design of TOKEN database records is discussed in detail below.

3. Application Servers

The Application servers are Web servers that do the business end of the user transaction. The Welcome Server's last task, after a successful
30 authentication, is to send a service selection screen to the user. The service selection screen contains the new multi-use TOKEN.

-128-

When the user selects a service, the selection request, with its embedded TOKEN, is sent to the appropriate Application Server. The Application Server validates the TOKEN using the Token Server **454** and, if valid, serves the request. A Token Server can authenticate a TOKEN issued by any one of the Token Servers on the same physical site. This is possible because the Token Servers **454** are database clients for the data maintained on a single database repository behind the corporate firewall.

- 10 An invalid TOKEN (or a missing TOKEN) always leads to the "Access Denied" page. This page is served by the Welcome Server(s) **450**. All denial of access attempts are logged.

The actual operation of the Application Server depends on the Application itself. The Application Servers in the DMZ are mapped to
15 <appName><num>.galileo.mci.com. Thus, in an embodiment with multiple applications (e.g., Profile Management, Message Center, Start Card Profile, Personal Web Space etc.), the same Welcome and Token servers **450** and **454** are used and more Applications servers are added as necessary.

- 20 Another embodiment adds more servers for the same application. If the work load on an application server increases beyond its capacity, another Application Server is added without any changes to existing systems. The SERVERS and TOKEN_HOSTS databases (described below) are updated to
25 add the record for the new server. The <num> part of the host name is used to distinguish the Application Servers.

There is no need to use DNS Round-robin on these names. The Welcome server **450** uses a configuration table (The SERVERS database loaded at
30 startup) to determine the Application Server name prior to sending the service selection screen.

B. Web Server System Environment

All the Web servers run the Netscape Commerce Server HTTP daemon. The Welcome Servers **450** run the daemon in normal as well as secure mode, while the Application Servers only run the secure mode daemon.

5

The Token Server(s) run a TCP service that runs on a well known port for ease of connection from within the DMZ. The Token Service daemon uses tcp_wrapper to deny access to all systems other than Welcome and Application server(s). In order to speed this authentication process, the list of addresses is loaded by these servers at configuration time, instead of using reverse name mapping at every request. The use of tcp_wrapper also provides the additional tools for logging Token Service activity.

10

The Application servers mostly work as front-ends for database services behind the firewall. Their main task is to validate the access by means of the TOKEN, and then validate the database request. The database requests are to Create, Read, Update or Delete exiting records or data fields on behalf of the user. The Application Servers do the necessary validation and authority checks before serving the request.

20

1. Welcome Servers

The Welcome Servers serve the HTML pages described below to the user at appropriate times. The pages are generated using Perl-based Common Gateway Interface (CGI) scripts. The Scripts reside in a directory which is NOT in the normal document-root directory of the HTTP daemon. The normal precautions regarding disabling directory listing and removing all backup files etc. are taken to ensure that CGI scripts are not readable to the user. Figure **41** shows the directory structure **455** on the Welcome Server **450**.

30

Figure **41** shows that the <document_root> **456** is separated from the

-130-

<server_root> 458. It also shows that the <document_root> directory holds only the welcome and access failure HTML pages.

5 The HTTP Server maps all requests to the "cgi" directory **460** based on the URL requested. The CGI scripts use the HTML templates from the "template" directory **462** to create and send the HTML output to the users on fly.

The use of the URL to map to a CGI script out of the <document_root> **456** blocks access to the <document_root> directory **456** by a malicious user.
10 Since every access to the Welcome Server **450** maps to a CGI script in the cgi directory **460** of the Welcome Server **450**, security is ensured by calling the authentication function at start of every script.

15 The user Authentication libraries are developed in Perl to authenticate the user identity. NSAPI's authentication phase routines also add features for TOKEN verification and access mode detection in the servers themselves.

The Welcome Servers **450** read their operating parameters into their environment from the database **456** at startup. It is necessary to keep this
20 information in the common database in order to maintain the same environment on multiple Welcome Servers **450**.

a) Welcome Page

25 The welcome page is sent as the default page when the Welcome Server **450** is first accessed. This is the only page that is not generated using a cgi script, and it is maintained in the <document_root> directory **456**. This page does the following:

- Confirms that the browser can display Frames. If the browser fails to display Frames correctly, this page will display an appropriate error
30 message and direct the user to down load Microsoft Internet Explorer V3.0 or later.

-131-

- Confirms that the browser can run Java. A failure will result in the user being directed to Microsoft Internet Explorer V3.0 or later.
- If the browser successfully displays Frames and runs Java, then this page will automatically request the Welcome Server 450 to send a login page.

The last action by the Welcome page is done using the Java applet embedded in page. This also switches the user's browser from normal to secure mode.

b) Login Page

The Login Page is a cgi-generated page that contains an embedded single use TOKEN, a Java applet, and form fields for the user to enter a User Id and Passcode. The page may display a graphic to emphasize service.

The processing of this page is padded to introduce an artificial delay. In the initial embodiment, this padding is set to zero.

The response from this page contains the TOKEN, a scrambled TOKEN value generated by the applet, User Id and Passcode. This information is sent to the Welcome server using a POST HTTP request by the Java applet. The POST request also contains the Applet signature.

If the login process is successful the response to this request is the Server Selection page. A failure at this stage results in an Access Failed page.

c) Server Selection Page

The Server Selection Page is a cgi-generated page which contains an embedded multi-use TOKEN. This page also shows one or more graphics to indicate the types of services available to the user. Some services are not accessible by our users. In other embodiments, when more than one service

-132-

exists, a User Services Database keyed on the User Id is used to generate this page.

5 The Welcome server uses its configuration information to embed the names of appropriate Application Servers with the view to sharing the load among all available Application Servers. This load sharing is done by using the configuration data read by the Welcome Server(s) during startup.

10 The Welcome Server selects an Application Server based upon entries in its configuration file for each of the services. These entries list the names of Application Server(s) for each application along with their probability of selection. This configuration table is loaded by the Welcome Servers at startup.

15 **d) Access Failed Page**

The Access Failed Page is a static page. That displays a message indicating that the login failed because of an error in User Id, Passcode or both. This page automatically loads the Login Page after a delay of 15 seconds.

20 **e) Access Denied Page**

The Access Denied Page is a static page that displays a message indicating that an access failed due to authentication error. This page automatically loads the Login Page after a delay of 15 seconds. The Access Denied page is called by the Application Servers when their authentication service fails to
25 recognize a TOKEN. All loads of this page will be logged and monitored.

2. Token Servers 454

The TOKEN service on the Web site is the only source of TOKEN generation and authentication. The Tokens themselves are stored in a shared Database

-133-

456. This database can be shared among all Token servers. The Token Database is behind the firewall out of the DMZ.

The Token service provides the services over a well-known (>1024) TCP port.

5 These services are provided only to a trusted host. The list of trusted hosts is maintained in a configuration database. This database is also maintained behind the firewall outside of the DMZ. The Token servers read their configuration database only on startup or when they receive a signal to refresh. The Token services are:

- 10
- Grant a single use TOKEN for login attempt.
 - Validate a single use TOKEN.
 - Validate a TOKEN.
 - Re-Validate a TOKEN.

15 TOKEN aging is implemented by a separate service to reduce the work load on the Token servers.

All access to the Token Server(s) is logged and monitored. The Token Service itself is written using the tcp_wrapper code available from MCI's internal security groups.

20 3. Profile Management Application Servers

The profile management application server(s) are the only type of Application servers implemented in the first embodiment. These servers have the same directory layout as the Welcome Servers. This allows the same system system to be used for both services if necessary.

25

C. Security

The data trusted by subscribers to the Web server is sensitive to them. They would like to protect it as much as possible. The subscribers have access to this sensitive information via the Web server(s). This
30 information may physically reside on one or more database servers, but as

-134-

far as the subscribers are concerned it is on Server(s) and it should be protected.

Presently only the following information needs to be protected in an
5 embodiment:

In other embodiments, profile information for directline account additional information is protected, including Email, Voice Mail, Fax Mail, and Personal Home Page information.

10

The protection is offered against the following type of attackers:

- People with access to Web;
- Other subscribers;
- MCI personnel;
- 15 • People with access to Subscriber's network;
- People with access to Subscriber's system;
- People looking over the shoulder of the Subscriber; and
- Other systems pretending to be Server(s).

20 The project implements the security by using the following schemes:

- Single use TOKENS for login attempts;
- Validated TOKENS will accompany all transactions;
- TOKEN aging to invalidate a TOKEN if it has not been used for ten minutes;
- 25 • TOKEN is associated with the IP Address of the calling machine, so TOKEN stealing is not an easy option;
- Use of SSL prevents TOKEN or DATA stealing without having physical access to the customer's display;
- Use of TOKEN in a form analogous to the Netscape Cookie gives us the
- 30 option to switch to cookies at a later date. Cookies offer us the facility to hide the TOKEN even further into the document for one extra layer of security; and

-135-

- Use of Hostile-IP table to block multiple offenders without detection by them.

5 In addition to the security implemented by TOKEN as described above, the Web Server(s) are in a Data Management Zone for further low level security. The DMZ security is discussed below.

D. Login Process

10 Figure 42 shows the Login Process. The sequence of events leading to a successful login is:

1. The user requests a connection to www.galileo.mci.com.
2. A server is selected from a set using DNS Round-robin.
3. An HTML Page is sent to the user's browser.
4. The Page checks the browser for JAVA Compliance and displays a
15 welcome message.
5. If the browser is not Java compliant, the process stops with an appropriate message.
6. If the browser is Java compliant, it automatically issues a "GET Login
20 Screen" request to the www.galileo.mci.com server. This request also switches the browser to SSL v2. It will fail if the Browser is not SSL compliant.
7. The Web Server does the following:
 - A. The Web server gets a Single Use Token from its internal Token service.
 - 25 B. The Web server picks one applet from a large set.
 - C. The Web server Records the Applet, Token, and Client IP address in a Database.
 - D. The Web server sends back the Login Screen, with Applet & Token.
- 30 8. User fills in the Login Screen fields - User Id and Passcode.

-136-

- A. The User Id is the user's Directline number (printed on User's Business cards and is in public domain).
 - B. The Passcode is a Six digit number known only to the User.
9. When the User presses Enter (or clicks on the LOGIN button) the Java Applet sends the UserId, Passcode, Token, and Scrambled Token back. The Scrambling Algorithm is specific to the Applet that was sent in Step **7D**.
10. If the browser's IP address is in the Hostile-IP table, the server goes back to Step **7**.
- 10 11. The Web server authenticates the Login request against what it recorded in Step **7C**.
12. If the test is invalid: if this is the third successive failed attempts from the same IP address server records the Address in Hostile-IP table.
13. The server goes back to Step **7**.
- 15 14. If the test is valid; The server sends a select services screen to the Browser with an embedded Token. The Token is still associated with the Browser's IP address, but it now has an expiration time.

E. Service Selection

- 20 When the user selects an option from the Service selection screen, the request is accompanied by the Token. The token is validated before the service is accessed, as shown in Figure **43**.

F. Service Operation

- 25 The screens generated by the Application Servers all contain the Token issued to the user when the Login process was started. This Token has an embedded expiration time and a valid source IP Address. All operation requests include this token as a part of the request.
- 30 The service requests are sent by the browser as HTML forms, APPLET based

-137-

forms or plain Hyper Links. In the first two instances, the Token is sent back as a Hidden field using the HTTP-POST method. The Hyper-Links use either the HTTP-GET method with embedded Token or substitute the Cookie in place of a Token. The format of the Token is deliberately chosen to be

5 compatible with this approach.

1. NIDS Server

The NIDS server in the system is isolated from the Web Servers by a router-based firewall. The NIDS server runs the NIDSCOMM and ASCOMM services
10 that allow TCP clients access to databases on the NIDS server. The NIDSCOMM and ASCOMM services do not allow connectivity to databases not physically located on the NIDS Server.

The following databases (C-tree services) on the NIDS server are used by the
15 Welcome Server, Token Server and Profile Management Application Server:

- 800_PIN_1CALL (this is a partitioned database);
- 1CALL_TRANS;
- COUNTRY;
- COUNTRY_SET;
- 20 • COUNTRY2 (maybe);
- COUNTRY_CITY (maybe);
- NPA_CITY;
- NPACITY_OA300 (maybe); and
- OP153T00.

25

In addition to the C Tree services named above the following new C tree services will be defined in the SERVDEF and used only on the NIDS server dedicated to the system:

- TOKEN;
- 30 • SERVERS;
- HOSTILE_IP;

-138-

- TOKEN_HOSTS; and
- SERVER_ENV.

The following descriptions for these databases do not show the filler field required at the first byte of each record, nor do they attempt to show any other filler fields that may be required for structure alignment along the 4-byte boundaries. This omission is made only for clarity. The numbers in parentheses next to the field definitions are the number of bytes required to hold the field value.

2. TOKEN database service.

The TOKEN database service is accessed by the Token Servers. The primary operations on this service are Create a new record, read a record for a given Token value and update a record for the given Token value.

A separate chron job running on the NIDS Server itself also accesses this database and deletes obsolete records on a periodic basis. This chron job runs every hour. It does a sequential scan of the database and deletes records for expired tokens.

The TOKEN database service contains the TOKEN records. The TOKEN records use a single key (the TOKEN) and have the following fields:

1. Version (1);
2. Use Flag (Single/Multi) (1);
3. Token Value (16);
4. IP Address (16);
5. User Id (16);
6. Time Granted (4); and
7. Time expires (4).

-139-

The key field is the Token Value.

3. SERVERS database service.

The Servers Database Service is accessed by the Welcome Server at configuration time. The records in this database contain the following fields:

- 5 1. Application Name (16);
2. Application Server Host Name (32);
3. Application Server Domain Name (32);
4. Weight (1);
5. Application Icon File URL (64); and
- 10 6. Application Description File URL (64).

The key field is the combination of Application Name, Server Host Name, and Server Domain Name. This database is read by the Welcome Servers sequentially. This database is also accessed by the Web Administrators to Create, Read, Update and Delete records. This access is via the ASCOMM
15 interface. The Web Administrators use the a HTML form and CGI script for their administration tasks.

4. HOSTILE_IP database service.

This database is accessed by the Welcome servers to create new records or
20 read existing records based on IP address as the key. The read access is very frequent. This database contains the following fields:

1. IP Address (16);
2. Time entered (4); and
3. Time expires (4).

25 The key field is the IP Address. All three values are set by the Welcome Server when creating this record. If the entry is to be over-ridden, the service doing the over-ride will only be allowed to change the Time expires value to <epoch_start>, thus flagging the entry as over-ride.

-140-

This database is also accessed by the Web Administrators to Create, Read, Update, and Delete records. Access is via the ASCOMM interface. The Web Administrators use the HTML form and CGI script for their administration tasks.

5

Customer Service uses a specially developed tool to access this database and access is allowed only from within the corporate firewall.

10 A chron job running on the NIDS server also accesses this database and deletes all obsolete records from this database. This job logs all its activity. The log of this job is frequently examined by the Web Administrators all the time.

5. TOKEN_HOSTS database service.

15 This database service lists IP Addresses of the hosts trusted by the Token Servers. This database is read by the Token Service at configuration time. The records in this database contain the following fields:

1. IP Address (16);
2. Authority (1);
- 20 3. Host Name (32);
4. Host Domain Name (32); and
5. Host description (64).

The key field is the IP Address. The Authority binary flag determines the access level. The low access level only allows validate/re-validate commands
25 on an existing TOKEN; the high access level additionally allows Grant and Validate single use TOKEN commands as well.

This database is also accessed by the Web Administrators to Create, Read, Update and Delete records. Access is via the ASCOMM interface. The Web
30 Administrators use the HTML form and CGI script for their administration

-141-

tasks.

6. SERVER_ENV database service.

This database is read by the Welcome and Application servers at startup. It

- 5 defines the starting environment for these servers. In one embodiment, only one field (and only for the Welcome Servers) is designed to be used. This is expanded in other embodiments.

The records in this database contain the following fields:

- 10 1. Sequence Number (4);
2. Application Name (16);
3. Environment Name (32); and
4. Environment Value (64).

- 15 The key field is Sequence Number. Environment values may refer to other environment variables by name. The values are evaluated at run time by the appropriate CGI scripts. The Welcome Servers are assigned the pseudo Application Name of WELCOME.

- 20 This database is also accessed by the Web Administrators to Create, Read, Update and Delete records. This access is via the ASCOMM interface. The Web Administrators use the HTML form and CGI script for their administration tasks.

25 7. Chron Job(s)

The NIDS Server runs a cleanup chron job. This job is scheduled to run every hour. The main tasks for this job are the following:

1. Scan the HOSTILE_IP database and report on all records. This report contains all records. The aim to track repeat offenders based on this
30 report.

-142-

2. Scan the HOSTILE_IP database and report on records with
<epoch_time> as their expiration time.
3. Scan the HOSTILE_IP database and delete obsolete records.
4. Scan the TOKEN database and report on all records. This report
5 format will be geared towards traffic reporting rather than scanning
each entry.
5. Scan the TOKEN database to delete obsolete records.

G. Standards

10 The following coding standards have been developed:

1. HTML Look and Feel standards;
2. Java Look and Feel standards (derived from the HTML look and feel
standards, these are the new class libraries used in development to
force a common look and feel on the site's pages); and
- 15 3. HTML Programming standards.

H. System Administration

The system administration tasks require reporting of at least the following
System Operating Parameters to the System Administrators:

- 20 • System stats and disk usage with time stamps;
- Network operating parameters with time stamps;
- Web page usage and access statistics with time stamps;
- TOKEN usage statistics;
- Hostile IP alarms and statistics;
- 25 The following tools and utilities are on the Servers in DMZ;
- Time synchronization;
- Domain Name Servers;
- System Log Monitoring;
- Alarm reporting; and
- 30 • Secure Shell.

-143-

The system generates alarms for the following conditions:

- Incorrect use of TOKENS;
- Hostile IP table changes;
- TOKEN Expiration; and
- 5 • Login attempts.

The alarms will be generated at different levels. The Web Servers use the following broad guidelines:

1. The servers run in a root environment.
- 10 2. The administrators are able to start a staging server on a non-standard port to test a new (staged) service.
3. The staging server is accessible from Internet during the staging run.
4. The Administrators have the option to move the staging software from staging area to production area with a single command. There are
- 15 suitable checks to make sure this is not done accidentally.

I. Product/Enhancement

A preferred embodiment enables directlineMCI customers additional control over their profile by providing a graphical user interface, and a common
20 messaging system. The capability to access the power of a preferred embodiment exists in the form of a directlineMCI profile and common messaging system. The user is able to modify his account, customizing his application by making feature/functionality updates. The application enables the power of the future capabilities that a preferred embodiment
25 integration will provide by allowing the user to run his application.

The user is able to access all of his messages by connecting with just one location. FAX, email, page and voice messages will be accessed through a centralized messaging interface. The user is able to call into the centralized
30 messaging interface through his message center interface to retrieve messages. A centralized message interface provides the user the capability to

-144-

manage his communications easily and effectively.

The user interface has two components, the user's application profile and message center. The interface is accessible through PC software (i.e., PC Client messaging interface), an ARU or a VRU, and a World Wide Web (WWW) Browser. The interface supports the customization of applications and the management of messages.

The feature/functionality requirements for an embodiment will be presented below. The first piece to be described is the ARU interface and its requirements for the user interface, message management and profile management. Following the ARU requirements, requirements are also provided for the WWW Browser and PC Client interfaces.

J. Interface Feature Requirements (Overview)

A front-end acts as an interface between the user and a screen display server in accordance with a preferred embodiment. The user is able to access the system and directly access his profile and messages. The user interface is used to update his profile and to access his messages. The user's profile information and the user's messages may reside in different locations, so the interface is able to connect to both places. Profile and messaging capabilities are separate components of the interface and have different requirements.

Through his interface, the user is able to update his profile in real-time through profile management. The application profile is the front-end to the user account directory, which is where all of the user account information resides in a virtual location. Also, a user is able to manage his messages (voicemail, faxmail, email, pager recall) through his message center. The message center is the front-end to the centralized messaging database, which is where all of the user's messages may reside, regardless of message

-145-

content.

Three user interfaces are supported:

- DTMF access to an ARU or VRU;
- 5 • WWW Browser access to a WWW Site; and
- PC Client access to a Messaging Server.

From the ARU, the users are able to update their profiles (directlineMCI only), retrieve voicemail messages and pager recall messages, and retrieve
10 message header (sender, subject, date/time) information for faxmail and email messages. Through the PC Client, the user is limited to message retrieval and message manipulation. The WWW Browser provides the user a comprehensive interface for profile management and message retrieval. Through the WWW Browser, the users are able to update their profiles
15 (directlineMCI, Information Services, List Management, Global Message Handling and Personal Home Pages) and retrieve all message types.

1. The User Account Profile

The user is able to access account information through the application
20 profile. The application profile provides an intelligent interface between the user and his account information, which resides in the user account directory. The User Account Directory accesses the individual account information of users. Users are able to read and write to the directory, making updates to their accounts. The directory allows search capabilities,
25 enabling customer service representatives to search for a specific account when assisting a customer.

When a customer obtains a phone number, the user account directory reflects the enrollment, and the user is able to access and update features
30 through his user account profile. If a customer withdraws, the user directory will reflect the deactivation, and the service will be removed from

-146-

the user's application profile.

In summary, the user account directory provides account information for each of the user's services. However, the user account directory is limited to:
5 directlineMCI profile, Information Services profile, Global Message Handling, List Management and Personal Home Page profiles. This information determines the feature/functionality of the user's application and provides the user with the flexibility that is necessary to customize his application, allowing MCI to meet his continuously changing communication needs.

10

2. The Database of Messages

An important feature that is offered is the integration of messages.

Messages of similar and dissimilar content are consolidated in one virtual location. Through a call, the message center provides the user with a review
15 of all of his messages, regardless of content or access. Through the interface messaging capabilities, the user is also able to maintain an address book and distribution lists.

This message database is a centralized information store, housing messages
20 for users. The message database provides common object storage capabilities, storing data files as objects. By accessing the message database, users retrieve voicemail, faxmail, email and pager recall messages from a single virtual location. In addition, by using common object storage capabilities, message distribution is extremely efficient.

25

K. Automated Response Unit (ARU) Capabilities

1. User Interface

The ARU interface is able to perform directlineMCI Profile Management, Information Services Profile Management, message retrieval and message

-147-

distribution. The DTMF access provided through the ARU is applied consistently across different components within the system. For example, entering alphabetic characters through the DTMF keypad is entered in the same manner regardless if the user is accessing Stock Quote information or broadcasting a fax message to a distribution list.

Voicemail Callback Auto Redial provides the capability to prompt for and collect a DTMF callback number from a guest leaving a voicemail and automatically launch a return call to the guest call back number when retrieving messages. Upon completing the callback, the subscriber will be able to return to the same place where they left off in the mailbox.

Music On-Hold provides music while a guest is on-hold.

Park and Page provides a guest an option to page a directlineMCI subscriber, through the directlineMCI gateway, then remain on-hold while the subscriber is paged. The subscriber receives the page and calls their directlineMCI number, where they can select to be connected with the guest on hold. Should the subscriber fail to connect a call with the guest, the guest will receive an option to be forwarded to voicemail. If the subscriber does not have voicemail as a defined option, then the guest a final message will be played for the guest.

Note: The guest has the ability to press an option to be forwarded to voicemail at any time while on hold.

Call Screening with Park and Page An embodiment provides the subscriber with functionality for responding to a park and page, the identity of the calling party (i.e., guest). This provides the subscribers the ability to choose whether they wish to speak to the guest or transfer the guest to voicemail, prior to connecting the call. Specifically, guests are ARU prompted to record their names when they select the park and page option. When the subscriber respond to the park and page, they will hear an ARU

-148-

prompt stating, "You have a call from RECORDED NAME", then be presented with the option to connect with the calling party or transfer the party to voicemail. If the subscriber does not have voicemail as a defined option, then the guest will be deposited to a final message. The guest also
5 will have the ability to press an option to be forwarded to voicemail at any time while on hold.

Two-way Pager Configuration Control and Response to Park and Page

The system also allows a subscriber to respond to a park and page
10 notification by instructing the ARU to route the call to voicemail or final message or continue to hold, through a command submitted by a two-way pager.

-149-

Text Pager Support

The system allows a subscriber to page a directlineMCI subscriber, through the directlineMCI gateway, and a leave a message to be retrieved by a text pager. Specifically, upon choosing the appropriate option, the guest will be
5 transferred to either the networkMCI Paging or the SkyTel message center where an operator will receive and submitcreate a text-based message to be retrieved by the subscriber's text pager.

Forward to the Next Termination Number

10 The system provides the capability for the party answering the telephone, to which a directlineMCI call has been routed, to have the option to have the call routed to the next termination number in the directlineMCI routing sequence. Specifically, the called party will receive a prompt from the directlineMCI ARU gateway, which indicates that the call has been routed to
15 this number by directlineMCI and providing the called party with the option to receive the incoming call or have the call routed to the next termination number or destination in the routing sequence. The options presented to a called party include:

- Press an option to accept the call
- 20 • Press an option to send the call to the next termination
- Let the call time-out (i.e., no action taken) and then proceed to the next termination.

Less Than 2 Second # Reorigination

An embodiment also provides the capability to reoriginate an outbound call,
25 from the directlineMCI gateway, by pressing the pound (#) key for less than two seconds. Currently, directlineMCI requires the # key to be depressed for two seconds or more before the subscriber can reoriginate a call.

L. Message Management**1. Multiple Media Message Notification**

30 The subscriber can receive an accounting of current messages across a

-150-

number of media, to include voicemail, faxmail, email, paging. Specifically, the subscriber will hear an ARU script stating, for example, "You have 3 new voicemail messages, 2 new faxmail messages, and 10 new email messages."

5 2. Multiple Media Message Manipulation

A subscriber is allowed to access the Universal Inbox to perform basic message manipulation, of messages received through multiple media (voicemail, faxmail, email, paging), through the directlineMCI ARU gateway. Subscribers are able to retrieve voicemail messages and pager messages,
10 and retrieve message header (priority, sender, subject, date/time, size) information for faxmail and email messages. In addition, subscribers are able to save, forward or delete messages reviewed from the ARU interface. The forward feature is limited to distributing messages as either voicemails or faxmails. Only voicemail messages can be forwarded as voicemails. Email,
15 faxmail and pager messages can be forwarded as faxmails; however, it may be necessary to convert email and pager messages to a G3 format. When forwarding messages as faxmails, subscribers have the ability to send messages to distribution lists and Fax Broadcast lists.

20 3. Text to Speech

The system converts text messages, received as email, faxmail or pager messages, into audio, which can be played back through the directlineMCI gateway. Initially, the text-to-speech capability will be limited to message header (priority, sender, subject, date/time, size) information.

25

Subscribers are provided the option to select whether they want to hear message headers first and then select which complete message they want to be played. The only message type that does not support a text-to-speech capability for the complete message will be faxmail messages. The capability
30 only exists to play faxmail headers. FAXmail header information includes

-151-

sender's ANI, date/time faxmail was received and size of faxmail.

4. Email Forwarding to a Fax Machine

Subscribers can forward an email, retrieved and reviewed through the
5 directlineMCI ARU gateway, to a subscriber-defined termination number.
Specifically, the subscriber has the ability to review an email message
through the directlineMCI ARU. After reviewing the message, the subscriber
receives, among the standard prompts, a prompt requesting whether he
would like to forward the email message to a specified termination number
10 or have the option to enter an impromptu number. Upon selecting this
option and indicating the termination number, the email message is
converted to a G3 format and transmitted to the specified termination
number. Email attachments that are binary files are supported. If an
attachment cannot be delivered to the terminating fax machine, a text
15 message must be provided to the recipient that the binary attachment could
not be forwarded. Forwarding of emails to a fax machine does not result in
the message being deleted from the "universal inbox".

5. Pager Notification of Messages Received

20 A subscriber can receive a pager notification, on a subscriber-defined
interval, indicating the number of messages, by message media, that
currently reside in the subscriber's "universal inbox". Specifically, the
subscriber will have the ability to establish a notification schedule, through
the directlineMCI ARU, to receive a pager message which indicates the
25 number of voicemail, faxmail, email and pager messages that reside in the
subscriber's "universal inbox".

6. Delivery Confirmation of Voicemail

The system provides the subscriber the ability to receive a confirmation

-152-

voicemail message when a subscriber-initiated voicemail message was not successfully delivered to the terminating party(s).

7. Message Prioritization

- 5 The system provides the guest the ability to assign either regular or urgent priority to a message. When the subscriber receives an accounting of messages, the prioritization will be indicated, and all urgent messages will be indexed before regular messages. This requirement only applies to voicemails, not faxmails. This will require that the "universal inbox" present
10 the proper message priority for directlineMCI voicemails.

M. Information Services

Through the ARU interface, users will be able to receive content from information services which are configurable through the WWW Browser
15 interface. Information content will be provided as an inbound service and an outbound service. The information content that is defined through the WWW Browser (i.e., Profile Management) is defined as the inbound information content and will be limited to:

- Stock Quotes and Financial News
- 20 • Headline News.

Subscribers also have the ability to access additional information content through the ARU interface; however, this information is not configurable through the WWW Browser (i.e., Profile Management). This additional
25 information content will be referred to as outbound information content and will consist of:

- Stock Quotes and Financial News;
- Headline News;
- Weather;
- 30 • Sports News and Scores;

-153-

- Soap Opera Updates;
 - Horoscopes;
 - Lottery Results;
 - Entertainment News; and
- 5 • Traveler's Assist.

The configurable parameters of the inbound information content is defined below. Retrieval of outbound information content will support the entry of alphabetic characters through a DTMF keypad. Entering of alphabetic
10 characters must be consistent with the manner that alphabetic characters are entered through DTMF for list management.

Access to Traveler's Assist will be bundled with the other outbound information services such that the subscriber only has to dial a single
15 800/8XX number. The 800/8XX call may extend to different termination depending upon the information content selected.

N. Message Storage Requirements

The message storage requirements are consistent with the message storage
20 requirements defined below.

O. Profile Management

directlineMCI Profile Management

Subscribers can also review, update and invoke their directlineMCI account
25 profiles. The directlineMCI profile management capabilities through the ARU interface are consistent with the presentation provided through the WWW Browser and support the following requirements:

- Create new directlineMCI profiles and assign names to the profile;
 - Invoke directlineMCI profiles;
- 30 • Voice annotate directlineMCI profile names;

-154-

- Update existing directlineMCI profiles;
- Support the rules-based logic of creating and updating directlineMCI profiles (e.g., selection of only one call routing option, like voicemail, will invoke override routing to voicemail; and updates made in one parameter must ripple through all affected parameters, like paging notification);
- Enable a directlineMCI number;
- Enable and define override routing number; and
- Enable and define FollowMe routing.
- Enable and define final routing (formerly called alternate routing) to:
 - Voicemail and pager;
 - Voicemail only;
 - Pager only;
 - Final message;
 - Invoke menu routing if two or more of the call routing options (FollowMe, voicemail, faxmail or pager) are enabled;
 - Define the default number for faxmail delivery;
 - Activate paging notification for voicemail;
 - Activate paging notification for faxmail; and
 - Provide guest option to classify voicemails for urgent delivery;
- Define call screening parameters for:
 - Name and ANI;
 - ANI only;
 - Name only; and
 - Enable or disable park and page.

P. Call Routing Menu Change

The system also provides the capability for subscribers to modify their call routing termination numbers without having to re-enter termination numbers which they do not wish to change. Specifically, the directlineMCI routing modification capability requires the subscriber to re-enter all termination numbers in a routing sequence should they wish to change any

-155-

of the routing numbers. This capability permits the subscriber to change only the termination numbers they wish to change, and indicate by pressing the “#” key when they do not wish to change a specific number in the routing sequence.

5

Q. *Two-way Pager Configuration Control and Response to Park and Page*

The system can also enable or disable predefined directlineMCI profiles through a command submitted by a two-way pager.

10

R. *Personalized Greetings*

The system provides subscribers the ability to review and update the personalized greeting that will be played from the ARU or displayed from their Personal Home Page. Each greeting is maintained separately and customized to the features available through each interface (ARU or Personal Home Page).

15

S. *List Management*

The system also provides the subscriber the ability to create and update lists, and create a voice annotation name for a list. Fax Broadcast list management capabilities are integrated with directlineMCI list management capabilities to provide a single database of lists. From the ARU interface, subscribers have the ability to review, update, add or delete members on a list. In addition, subscribers are able to delete or create lists. The ARU interface is able to use the lists to distribute voicemail and faxmail messages.

20

25

Access to distribution lists supports alphabetic list names such that lists are not limited to list code names. Entering of alphabetic characters through

-156-

DTMF to the ARU for list names is consistent with the manner that alphabetic characters are entered through DTMF for Information Services. The List Management requirements are discussed in greater detail below.

- 5 In addition to providing message manipulation capabilities, the PC Client also provides an address book and access to lists. The user is able to make modifications to the address book and manage distribution lists for voice, fax, email and paging messages. In one embodiment, lists created or maintained through the PC Client interface are not integrated with lists
10 created or maintained through the WWW Browser or ARU interfaces, but such integration can be implemented in an alternative embodiment. The subscriber is able to send a message to a distribution list from the PC Client. This requires a two-way interface between the PC Client and the List Management database whereby the PC Client can export a comma delimited
15 or DBF formatted file to the database of lists.

The user is able to create and modify recipient address information through his interface PC software. The user is able to record multiple types of addresses in his address book, including 10 digit ANIs, voice mailbox ids,
20 fax mailbox ids, paging numbers and email addresses (MCIMail and Internet). This information should be saved onto the PC. The address information retained on the PC Client is classified and sorted by recipient's name.

25 **T. Global Message Handling**

From the ARU interface, subscribers are able to define which message types can be accessed from the "universal inbox". The global message handling requirements are consistent with the requirements defined below.

-157-

X. INTERNET TELEPHONY AND RELATED SERVICES

The discussion thus far has provided an introduction to the Internet, and therefore Internet telephony, but Internet telephony encompasses quite a few areas of development. The following is a summary of Internet telephony, divided into six key areas. The first area consists of access to Internet telephony services. This area involves accessing and utilizing the Internet using such mechanisms as satellites, dialup services, T1, T3, DS3, OC3, and OC12 dedicated lines, SMDS networks, ISDN B-channels, ISDN D-channels, multirate ISDN, multiple B-channel bonded ISDN systems, Ethernet, token ring, FDDI GSM, LMDS, PCS, cellular networks, frame relay, and X.25.

The second area involves sharing Internet telephony. Multimedia data can utilize circuit-switched networks quite readily due to the high reliability and throughput potential. Issues include shared data, pushing URL data between parties, data conferencing, shared whiteboarding, resource collaboration, and ISDN user-user signaling.

The third area deals with routing Internet telephony. Issues include the time-of-day, the day-of-week, the day-of-month, and the day-of-year, in addition to geographic points of origin, network point of origin, and time zone of origin. Analysis of routing also includes user data, destination parties, telephone numbers, lines of origin, types of bearer service, presubscribed feature routing, ANI, and IP addresses. Also, VNET plans, range privileges, directory services, and Service Control Points (SCP)s fall into routing Internet telephony.

The fourth category deals with quality of service. Analysis must include switched networks, ISDN, dynamic modifications, Internet telephony, RSVP, and redundant network services. In addition, this category includes hybrid Internet/telephony switches, Ethernet features, ISDN features, analog local loops and public phones, and billing for reserved and/or utilized services.

-158-

The fifth category is composed of directory services, profiles, and notifications. Examples are distributed directories, finding-me and follow-me services, directory management of telephony, and user interfaces.

- 5 Calling party authentication security is also included. Hierarchical and object-oriented profiles exist, along with directory service user profiles, network profile data structures, service profiles, and order entry profiles.

- 10 The sixth category consists of hybrid Internet telephony services. Areas include object directed messaging, Internet telephony messaging, Internet conferencing, Internet faxing, information routing (IMMR), voice communications, and intranets (such as those that exist within a company). Other services include operator services, management service, paging services, billing services, wireless integration, message broadcasts,
- 15 monitoring and reporting services, card services, video-mail services, compression, authorization, authentication, encryption, telephony application builders, billing, and data collection services.

- 20 The seventh category consists of hybrid Internet media services, which include areas of collaborative work which involve a plurality of users. Users can collaborate on Audio, Data and Video. This area includes media conferencing within the Hybrid network. Then there is a broadly related area of Reservations mechanism, Operator-assisted conferencing, and the introduction of content into conferences. The Virtual locations of these
- 25 conferences will assume importance in the future. The next-generation Chat Rooms will feature virtual conference spaces with simulated Office Environments.

-159-

A. System Environment for Internet Media

1. Hardware

A preferred embodiment of a system in accordance with the present invention is preferably practiced in the context of a personal computer such as the IBM PS/2, Apple Macintosh computer or UNIX based workstation. A representative hardware environment is depicted in Figure **1A**, which illustrates a typical hardware configuration of a workstation **99** in accordance with a preferred embodiment having a central processing unit **10**, such as a microprocessor, and a number of other units interconnected via a system bus **12**. The workstation shown in Figure **1A** includes a Random Access Memory (RAM) **14**, Read Only Memory (ROM) **16**, an I/O adapter **18** for connecting peripheral devices such as a communication network (e.g., a data processing network) **81**, printer **30** and a disk storage unit **20** to the bus **12**, a user interface adapter **22** for connecting a keyboard **24**, a mouse **26**, a speaker **28**, a microphone **32**, and/or other user interface devices such as a touch screen (not shown) to the bus **12**, and a display adapter **36** for connecting the bus **12** to a display device **38**. The workstation typically has resident thereon an operating system such as the Microsoft Windows NT or Windows/95 Operating System (OS), the IBM OS/2 operating system, the MAC System/7 OS, or UNIX operating system. Those skilled in the art will appreciate that the present invention may also be implemented on platforms and operating systems other than those mentioned.

2. Object-Oriented Software Tools

A preferred embodiment is written using JAVA, C, and the C++ language and utilizes object oriented programming methodology. Object oriented programming (OOP) has become increasingly used to develop complex applications. As OOP moves toward the mainstream of software design and development, various software solutions require adaptation to make use of

-160-

the benefits of OOP. A need exists for these principles of OOP to be applied to a messaging interface of an electronic messaging system such that a set of OOP classes and objects for the messaging interface can be provided.

- 5 OOP is a process of developing computer software using objects, including the steps of analyzing the problem, designing the system, and constructing the program. An object is a software package that contains both data and a collection of related structures and procedures. Since it contains both data and a collection of structures and procedures, it can be visualized as a self-
10 sufficient component that does not require other additional structures, procedures or data to perform its specific task. OOP, therefore, views a computer program as a collection of largely autonomous components, called objects, each of which is responsible for a specific task. This concept of packaging data, structures, and procedures together in one component or
15 module is called encapsulation.

In general, OOP components are reusable software modules which present an interface that conforms to an object model and which are accessed at run-time through a component integration architecture. A component
20 integration architecture is a set of architectural mechanisms which allow software modules in different process spaces to utilize each other's capabilities or functions. This is generally done by assuming a common component object model on which to build the architecture.

- 25 It is worthwhile to differentiate between an object and a class of objects at this point. An object is a single instance of the class of objects, which is often just called a class. A class of objects can be viewed as a blueprint, from which many objects can be formed.

- 30 OOP allows the programmer to create an object that is a part of another object. For example, the object representing a piston engine is said to have a composition-relationship with the object representing a piston. In reality,

-161-

a piston engine comprises a piston, valves and many other components; the fact that a piston is an element of a piston engine can be logically and semantically represented in OOP by two objects.

- 5 OOP also allows creation of an object that “derived from” another object. If there are two objects, one representing a piston engine and the other representing a piston engine wherein the piston is made of ceramic, then the relationship between the two objects is not that of composition. A ceramic piston engine does not make up a piston engine. Rather it is merely one
10 kind of piston engine that has one more limitation than the piston engine; its piston is made of ceramic. In this case, the object representing the ceramic piston engine is called a derived object, and it inherits all of the aspects of the object representing the piston engine and adds further limitation or detail to it. The object representing the ceramic piston engine
15 “derives from” the object representing the piston engine. The relationship between these objects is called inheritance.

- When the object or class representing the ceramic piston engine inherits all of the aspects of the objects representing the piston engine, it inherits the
20 thermal characteristics of a standard piston defined in the piston engine class. However, the ceramic piston engine object overrides these ceramic specific thermal characteristics, which are typically different from those associated with a metal piston. It skips over the original and uses new functions related to ceramic pistons. Different kinds of piston engines have
25 different characteristics, but may have the same underlying functions associated with them (e.g., number of pistons in the engine, ignition sequences, lubrication, etc.). To access each of these functions in any piston engine object, a programmer would identify the same functions with the same names, but each type of piston engine may have
30 different/overriding implementations of functions behind the same name. This ability to hide different implementations of a function behind the same name is called polymorphism and it greatly simplifies communication among

-162-

objects.

With the concepts of composition-relationship, encapsulation, inheritance and polymorphism, an object can represent just about anything in the real world. In fact, our logical perception of the reality is the only limit on determining the kinds of things that can become objects in object-oriented software. Some typical categories are as follows:

- Σ Objects can represent physical objects, such as automobiles in a traffic-flow simulation, electrical components in a circuit-design program, countries in an economics model, or aircraft in an air-traffic-control system.
- Σ Objects can represent elements of the computer-user environment such as windows, menus or graphics objects.
- Σ An object can represent an inventory, such as a personnel file or a table of the latitudes and longitudes of cities.
- Σ An object can represent user-defined data types such as time, angles, and complex numbers, or points on the plane.

With this enormous capability of an object to represent just about any logically separable matters, OOP allows the software developer to design and implement a computer program that is a model of some aspects of reality, whether that reality is a physical entity, a process, a system, or a composition of matter. Since the object can represent anything, the software developer can create an object which can be used as a component in a larger software project in the future.

If 90% of a new OOP software program consists of proven, existing components made from preexisting reusable objects, then only the remaining 10% of the new software project has to be written and tested from scratch. Since 90% already came from an inventory of extensively tested reusable objects, the potential domain from which an error could originate is 10% of the program. As a result, OOP enables software developers to build

-163-

objects out of other, previously built, objects.

This process closely resembles complex machinery being built out of assemblies and sub-assemblies. OOP technology, therefore, makes software engineering more like hardware engineering in that software is built from existing components, which are available to the developer as objects. All this adds up to an improved quality of the software as well as an increased speed of its development.

- 10 Programming languages are beginning to fully support the OOP principles, such as encapsulation, inheritance, polymorphism, and composition-relationship. With the advent of the C++ language, many commercial software developers have embraced OOP. C++ is an OOP language that offers a fast, machine-executable code. Furthermore, C++ is suitable for
- 15 both commercial-application and systems-programming projects. For now, C++ appears to be the most popular choice among many OOP programmers, but there is a host of other OOP languages, such as Smalltalk, common lisp object system (CLOS), and Eiffel. Additionally, OOP capabilities are being added to more traditional popular computer programming languages such
- 20 as Pascal.

The benefits of object classes can be summarized, as follows:

- Σ Objects and their corresponding classes break down complex programming problems into many smaller, simpler problems.
- 25 Σ Encapsulation enforces data abstraction through the organization of data into small, independent objects that can communicate with each other. Encapsulation also protects the data in an object from accidental damage, but allows other objects to interact with that data by calling the object's member functions and structures.
- 30 Σ Subclassing and inheritance make it possible to extend and modify objects through deriving new kinds of objects from the standard classes available in the system. Thus, new capabilities are created

-164-

without having to start from scratch.

Σ Polymorphism and multiple inheritance make it possible for different programmers to mix and match characteristics of many different classes and create specialized objects that can still work with related objects in predictable ways.

Σ Class hierarchies and containment hierarchies provide a flexible mechanism for modeling real-world objects and the relationships among them.

Σ Libraries of reusable classes are useful in many situations, but they also have some limitations. For example:

Σ Complexity. In a complex system, the class hierarchies for related classes can become extremely confusing, with many dozens or even hundreds of classes.

Σ Flow of control. A program written with the aid of class libraries is still responsible for the flow of control (i.e., it must control the interactions among all the objects created from a particular library). The programmer has to decide which functions to call at what times for which kinds of objects.

Σ Duplication of effort. Although class libraries allow programmers to use and reuse many small pieces of code, each programmer puts those pieces together in a different way. Two different programmers can use the same set of class libraries to write two programs that do exactly the same thing but whose internal structure (i.e., design) may be quite different, depending on hundreds of small decisions each programmer makes along the way. Inevitably, similar pieces of code end up doing similar things in slightly different ways and do not work as well together as they should.

Class libraries are very flexible. As programs grow more complex, more programmers are forced to reinvent basic solutions to basic problems over and over again. A relatively new extension of the class library concept is to have a framework of class libraries. This framework is more complex and

-165-

consists of significant collections of collaborating classes that capture both the small scale patterns and major mechanisms that implement the common requirements and design in a specific application domain. They were first developed to free application programmers from the chores
5 involved in displaying menus, windows, dialog boxes, and other standard user interface elements for personal computers.

Frameworks also represent a change in the way programmers think about the interaction between the code they write and code written by others. In
10 the early days of procedural programming, the programmer called libraries provided by the operating system to perform certain tasks, but basically the program executed down the page from start to finish, and the programmer was solely responsible for the flow of control. This was appropriate for printing out paychecks, calculating a mathematical table, or solving other
15 problems with a program that executed in just one way.

The development of graphical user interfaces began to turn this procedural programming arrangement inside out. These interfaces allow the user, rather than program logic, to drive the program and decide when certain
20 actions should be performed. Today, most personal computer software accomplishes this by means of an event loop which monitors the mouse, keyboard, and other sources of external events and calls the appropriate parts of the programmer's code according to actions that the user performs.

The programmer no longer determines the order in which events occur.
25 Instead, a program is divided into separate pieces that are called at unpredictable times and in an unpredictable order. By relinquishing control in this way to users, the developer creates a program that is much easier to use. Nevertheless, individual pieces of the program written by the developer still call libraries provided by the operating system to accomplish certain
30 tasks, and the programmer must still determine the flow of control within each piece after it's called by the event loop. Application code still "sits on top of" the system.

-166-

Even event loop programs require programmers to write a lot of code that should not need to be written separately for every application. The concept of an application framework carries the event loop concept further. Instead
5 of dealing with all the nuts and bolts of constructing basic menus, windows, and dialog boxes and then making these things all work together, programmers using application frameworks start with working application code and basic user interface elements in place. Subsequently, they build from there by replacing some of the generic capabilities of the framework
10 with the specific capabilities of the intended application.

Application frameworks reduce the total amount of code that a programmer must write from scratch. However, because the framework is really a generic application that displays windows, supports copy and paste, and so
15 on, the programmer can also relinquish control to a greater degree than event loop programs permit. The framework code takes care of almost all event handling and flow of control, and the programmer's code is called only when the framework needs it (e.g., to create or manipulate a data structure).

20 A programmer writing a framework program not only relinquishes control to the user (as is also true for event loop programs), but also relinquishes the detailed flow of control within the program to the framework. This approach allows the creation of more complex systems that work together in interesting ways, as opposed to isolated programs with custom code being
25 created over and over again for similar problems.

Thus, as explained above, a framework basically is a collection of cooperating classes that make up a reusable design solution for a given problem domain. It typically provides objects that define default behavior
30 (e.g., for menus and windows), and programmers use it by inheriting some of that default behavior and overriding other behavior so that the framework calls application code at the appropriate times.

-167-

There are three main differences between frameworks and class libraries:

Σ Behavior versus protocol. Class libraries are essentially collections of behaviors that you can call when you want those individual behaviors in your program. A framework, on the other hand, provides not only behavior but also the protocol or set of rules that govern the ways in which behaviors can be combined, including rules for what a programmer is supposed to provide versus what the framework provides.

Σ Call versus override. With a class library, the code the programmer instantiates objects and calls their member functions. It's possible to instantiate and call objects in the same way with a framework (i.e., to treat the framework as a class library), but to take full advantage of a framework's reusable design, a programmer typically writes code that overrides and is called by the framework. The framework manages the flow of control among its objects. Writing a program involves dividing responsibilities among the various pieces of software that are called by the framework rather than specifying how the different pieces should work together.

Σ Implementation versus design. With class libraries, programmers reuse only implementations, whereas with frameworks, they reuse design. A framework embodies the way a family of related programs or pieces of software work. It represents a generic design solution that can be adapted to a variety of specific problems in a given domain. For example, a single framework can embody the way a user interface works, even though two different user interfaces created with the same framework might solve quite different interface problems.

B. Telephony Over The Internet

Voice over the Internet has become an inexpensive hobbyist commodity.

30 Several firms are evolving this technology to include interworking with the PSTN. This presents both a challenge and an opportunity for established

-168-

carriers like MCI and BT especially in the IDDD arena. This discussion explores how a carrier class service could be offered based on this evolving technology. Of particular interest are ways to permit interworking between the PSTN and the Internet using 1 plus dialing.

5

The introductory discussion considers the technical requirements to support PC to PC connectivity in a more robust manner than presently offered, in addition to the technical requirements for a PSTN to Internet voice gateway. Consideration is given to how calls can be placed from PCs to a PSTN destination and visa versa. The case of PSTN to PSTN communications, using the Internet as a long distance network is also explored.

10

It is shown how such services can be offered in a way that will complement existing PSTN services, offering lower prices for a lower quality of service. At issue in the longer term is the steady improvement in quality for Internet telephony and whether this will ultimately prove competitive with conventional voice services.

15

1. Introduction

20

In the mid-late 1970s, experiments in the transmission of voice over the Internet were conducted as part of an ongoing program of research sponsored by the US Defense Advanced Research Projects Agency. In the mid-1980s, UNIX-based workstations were used to conduct regular audio/video conferencing sessions, in modest quantities, over the Internet.

25

These experimental applications were extended in the late 1980s with larger scale, one-way multicasting of voice and video. In 1995 a small company, VocalTec (www.vocaltec.com), introduced an inexpensive software package that was capable of providing two way voice communications between multimedia PCs connected to the Internet. Thus was born a new generation of telephony over the Internet.

30

-169-

The first software package, and its immediate followers, provided a hobbyist tool. A meeting place based on a Internet Relay Chat "room" (IRC) was used to establish point to point connections between end stations for the voice transfer. This resulted in chance meetings, as is common in chat rooms, or
5 a prearranged meeting, if the parties coordinated ahead of time, by email or other means.

a) How it Works

A user with a multi-media PC and an Internet connection can add the
10 Internet Telephony capability by loading a small software package. In the case of VocalTec, the package makes a connection to the meeting place (IRC server), based on a modified chat server. At the IRC the user sees a list of all other users connected to the IRC.

15 The user calls another user by clicking on his name. The IRC responds by sending the IP address of the called party. For dial in users of the Internet, an IP address is assigned at dial in time, and consequently will change between dial in sessions. If the destination is not already engaged in a voice connection, its PC beeps a ring signal. The called user can answer the
20 phone with a mouse click, and the calling party then begins sending traffic directly to the IP address of the called party. A multi-media microphone and speakers built into or attached to the PC are used as a speakerphone. The speaker's voice is digitized, compressed and packetized for transmission across the Internet. At the other end it is decompressed and converted to
25 sound through the PC's speakers.

b) Implications

Telephony over the Internet offers users a low cost service, that is distance and border insensitive. For the current cost of Internet access (at low hourly rates, or in some cases unlimited usage for a flat fee) the caller can hold a
30 voice conversation with another PC user connected to the Internet. The

-170-

called party contributes to the cost of the conversation by paying for his Internet access. In the case that one or both ends are LAN connected to the Internet by leased lines the call is free of additional charges. All of this is in contrast to the cost of a conventional long distance, possibly international,
5 call.

c) Quality of Service

The voice quality across the Internet is good, but not as good as typical telephone toll quality. In addition, there are significant delays experienced
10 during the conversation. Trying to interrupt a speaker in such an environment is problematic. Delay and quality variations are as much a consequence of distance and available capacity as they are a function of compression, buffering and packetizing time.

Delays in the voice transmission are attributable to several factors. One of
15 the biggest contributors to delays is the sound card used. The first sound cards were half duplex and were designed for playback of recorded audio. Long audio data buffers which helped ensure uninterrupted audio playback introduced real time delays. Sound card based delays are being reduced
20 over time as full duplex cards designed for "speakerphone" applications are brought to the market.

Other delays are inherent in the access line speeds (typically 14.4-28.8 kbps for dial-up internet access) and in the packet forwarding delays in the
25 Internet. Also there is delay inherent in filling a packet with digitized encoded audio. For example, to fill a packet with 90 ms of digitized audio, the application must wait at least 90 ms to receive the audio to digitize. Shorter packets reduce packet-filling delays, but increase overhead by increasing the packet header to packet payload data ratio. The increased
30 overhead also increases the bandwidth demands for the application, so that an application which

-171-

uses short packets may not be able to operate on a 14.4 kbps dial-up connection. LAN-based PCs suffer less delay, but everyone is subject to variable delays which can be annoying.

- 5 Lastly, there are delays inherent in audio codecs. Codec delays can vary from 5 to 30 ms for encoding or decoding. Despite the higher latencies associated with internet telephony, the price is right, and this form of voice communication appears to be gaining in popularity.

10 2. IP Phone as a Commercial Service

IP telephony technology is here whether the established carriers like it or not. Clearly the use of the Internet to provide international voice calls is a potential threat to the traditional International Direct Distance Dialing (IDDD) revenue stream. Although it may be several years before there is an
15 appreciable revenue impact, it cannot be stopped, except perhaps within national borders on the basis of regulation. The best defense by the carriers is to offer the service themselves in an *industrial strength* fashion. To do this requires an improved call setup facility and an interface to the PSTN.

20 Facilitating PC to PC connections is useful for cases in which the voice conversation needs to be conducted during a simultaneous Internet data packet communication, and the parties don't have access to separate telephone facilities. Dial-up Internet subscribers with only one access circuit might find themselves in that position. Cost considerations may also
25 play a role in dictating the use of PC to PC telephony. The larger use of this technology will occur when the Internet can be used in place of the long distance network to interconnect ordinary telephone hand sets. The number of multi-media Internet connected PCs in the world (estimated at 10 million) is minuscule compared to the number of subscriber lines worldwide
30 (estimated at 660 million). This service is in the planning stages of several companies.

-172-

In the sections below we look at each of the end point combinations possible in a full Internet telephony service. The most important aspects relate to the PSTN to Internet gateway capabilities. Of particular interest is the possibility of providing the PSTN caller with one-step dialing to his called party. The one-step dialing solutions discussed below are in the context of the North American numbering plan. There are essentially four cases:

1. PC to PC;
2. PC to PSTN;
- 10 3. PSTN to PC; and
4. PSTN to PSTN.

The first case is addressed by today's IP Phone software. The second and third case are similar but not identical and each requires a gateway between the PSTN and the Internet. The last case uses the Internet as a long distance network for two PSTN telephones.

a) PC to PC

(1) Directory Service

To facilitate PC to PC Internet Telephony a directory service is needed to find the IP address of the called party based on a name presented by the calling party. Early internet telephony software utilized a modified internet chat server as a meeting place. More recently, internet telephony software is replacing the chat server with a directory service which will uniquely identify internet telephone users (perhaps by email address). To receive calls, customers would register with the directory service (for a fee, with recurring charges) and would make their location (IP address) known to the directory system whenever they connect to the Internet and want to be available for calls. The best way to accomplish automatic notification is to get agreement between the vendors of IP phone software on a protocol to notify the directory service whenever the software is started (automatic presence notification). It would also be desirable, as an option, to find a way to

-173-

automatically invoke the IP phone software when the IP stack is started.

The directory service is envisioned as a distributed system, somewhat like the Internet Domain Name System, for scalability. This is not to imply, necessarily, the user@foo.com format for user identification.

Theoretically only the called parties need to be registered. If the calling party is not registered, then the charge for the call (if there is one) could be made to the called party (a collect call). Alternatively, we can insist that the caller also be registered in the directory and billed through that mechanism (this is desirable since we charge for the registration and avoid the complications that collect calls require). A charge for the call setup is billed, but not for the duration, over and above the usual Internet charges. Duration charges already apply to the dial up Internet user and Internet usage charges, both for dial up and dedicated usage, are probably not too far away.

Collect calls from a registered user may be required to meet market demand.

A scheme for identifying such calls to the called party must be devised, along with a mechanism for the called party to accept or reject the collect call. The directory service will track the ability of the called software to support this feature by version number (or, alternatively, this could be a matter for online negotiation between the IP telephony software packages).

In the event of collect calls (assuming the caller is not registered), the caller could claim to be anyone she chooses. The directory service will force the caller to take on a temporary "assigned" identity (for the duration of the call) so the called party will know this is an unverified caller. Since IP addresses are not necessarily fixed, one cannot rely on them to identify parties.

(2) Interoperability

Nearly all IP phone software packages on the market today use different voice encoding and protocols to exchange the voice information. To facilitate

-174-

useful connections the directory will store the type and version (and possibly options) of Internet phone software being used. To make this work effectively software vendors will report this information automatically to the directory service. This information will be used to determine interoperability when a call is placed. If the parties cannot interoperate, an appropriate message must be sent to the caller. As an alternative, or in addition to registration of software type, a negotiation protocol could be devised to determine interoperability on the fly, but all packages would have to "speak" it.

There is a question of whether translations between IP phone encoding can be performed with acceptable quality to the end user. Such a service could have a duration and or volume fee associated with it, which might limit the desirability of its use. Also, after a shake out period we expect only a few different schemes to exist and they will have interoperability, perhaps through an industry agreed lowest common denominator compression and signaling protocol. So far, all the IP phone software vendors we have contacted are in favor of an *Esperanto* that will permit interoperability. If this comes to pass the life span of the translation services will be short, probably making them not economically attractive.

We can help the major software vendors seek consensus on a "common" compression scheme and signaling protocol that will provide the needed interoperability. Once the major vendors support this method the others will follow. This is already happening, with the recent announcements from Intel, Microsoft, Netscape, and VocalTec that they will all support the H.323 standard in coming months. This can be automatically detected at call setup time. The directory service would keep track of which versions of which software can interoperate. To facilitate this functionality the automatic notification of presence should include the current software version. This way upgrades can be dynamically noted in the directory service. Some scheme must also be defined to allow registration information

-175-

to be passed between software packages so if a user switches packages she is able to move the registration information to the new application. There is no reason to object if the user has two applications each with the same registration information. The directory service will know what the user is currently running as part of the automatic presence notification. This will cause a problem only if the user can run more than one IP phone package at the same time. If the market requires this ability the directory service could be adapted to deal with it. The problem could also be overcome through the use of negotiation methods between interacting IP phone software packages.

10

(3) Call Progress Signaling

If the user is reachable through the directory system, but is currently engaged in a voice connection, then a call waiting message (with caller ID, something which is not available in the PSTN call waiting service) is sent to the called party and a corresponding message is sent back to the caller.

15

If the user is reachable through the directory system, but is currently not running his voice software (IP address responds, but not the application -- see below for verification that this is the party in question) then an appropriate message is returned to the caller. (As an option an email could be sent to the called party to alert him to the call attempt. An additional option would be to allow the caller to enter a voice message and attach the "voice mail" to the email. The service could also signal the caller to indicate: busy, unreachable, active but ignored call waiting, etc. Other notification methods to the called party can also be offered, such as FAX or paging. In each case, the notification can include the caller's identity, when known.) Once the directory system is distributed it will be necessary to query the other copies if contact cannot be made based on local information. This system provides the ability to have various forms of notification, and to control the parameters of those forms.

20
25
30

-176-

(4) Party Identification

A critical question is how will the directory service know that a called party is no longer where she was last reported (i.e., has "gone away"). The dialed in party might drop off the network in a variety of ways (dialed line dropped, PC hung, Terminal Server crashed) without the ability to explicitly inform the directory service of his change in status. Worse yet, the user might have left the network and another user with a voice application might be assigned the same IP address. (This is OK if the new caller is a registered user with automatic presence notification; the directory service could then detect the duplicate IP address. There may still be some timing problems between distributed parts of the directory service.) Therefore, some scheme must exist for the directory service to determine that the customer is still at the last announced location.

One approach to this is to implement a shared secret with the application, created at registration time. Whenever the directory system is contacted by the software (such as automatic presence notification or call initialization) or attempts to contact the called party at the last known location, it can send a challenge (like CHAP) to the application and verify the response. Such a scheme eliminates the need for announcing "I am no longer here", or wasteful keep alive messages. A customer can disconnect or turn off his IP phone application at any time without concern for notification to the directory system. If multiple IP phone applications are supported, by the directory service, each may do the challenge differently.

25

(5) Other Services

Encrypted internet telephone conversations will require a consensus from the software vendors to minimize the number of encryption setup mechanisms. This will be another interoperability resolution function for the directory service. The directory service can provide support for public key applications and can provide public key certificates issued by suitable

30

-177-

certificate authorities.

The user can also specify on the directory service, that his PC be called (dial out) if she is not currently on-line. Charges for the dial out can be billed to the called party, just as would happen for call forwarding in POTS. The call detail record (CDR) for the dial out needs to be associated with the call detail of an entity in the IP Phone system (the called party). Note that this is different than the PC to PSTN case in that no translation of IP encoded voice to PCM is required, indeed the dial out will use TCP/IP over PPP. If the dial out fails an appropriate message is sent back.

The dial out could be domestic or international. It is unlikely that the international case will exist in practice due to the cost. However, there is nothing to preclude that case and it requires no additional functionality to perform.

b) PC to PSTN

The PSTN to Internet gateway must support translating PCM to multiple encoding schemes to interact with software from various vendors. Alternatively the common compression scheme could be used once it is implemented. Where possible, the best scheme, from a quality stand point, should be used. In many cases it will be the software vendor's proprietary version. To accomplish that, telcos will need to license the technology from selected vendors. Some vendors will do the work needed to make their scheme work on telco platforms.

(1) Domestic PSTN Destination

The PC caller needs to be registered to place calls to the PSTN. The only exception to this would be if collect calls from the Internet are to be allowed. This will add complications with respect to billing. To call a PSTN destination the PC caller specifies a domestic E.164 address. The directory

-178-

system maps that address to an Internet dial out unit based on the NPA-NXX. The expectation is that the dial out unit will be close to the destination and therefore will be a local call. One problem is how to handle the case where there is no "local" dial out unit. Another problem is what to do if the "local" out dial unit is full or otherwise not available.

Three approaches are possible. One approach is to offer the dial out service only when local calls are possible. A second approach is to send a message back to the caller to inform him that a long distance call must be placed on his behalf and request permission to incur these charges. A third approach is to place the call regardless and with no notification. Each of these cases requires a way to correlate the cost of the dial out call (PSTN CDR) with the billing record of the call originator (via the directory service).

The third approach will probably add to the customer support load and result in unhappy customers. The first approach is simple but restrictive. Most users are expected to be very cost conscious, and so might be satisfied with approach one. Approach two affords flexibility for the times the customer wants to proceed anyway, but it adds complexity to the operation. A possible compromise is to use approach one, which will reject the call for the reason that no local out dial is available. We could also add an attribute in the call request that means "I don't care if this ends up as a long distance call." In this case the caller who was rejected, but wants to place the call anyway makes a second call attempt with this attribute set. For customers with money to spare, all PSTN calls could be made with that attribute set.

Placing domestic PSTN calls supports the international calling requirement for Internet originated calls from Internet locations outside the US.

(2) International PSTN Destinations

Calls to an international PSTN station can be done in one of two ways. First,

-179-

an international call could be placed from a domestic dial out station. This is not an attractive service since it saves no money over the customer making an international telephone call himself. Second, the Internet can be used to carry the call to the destination country and a "local" dial out can be made there.

This situation is problematic for it must be agreed to by the carrier at the international destination. This case may be viable in one of two ways. Both ways require a partner at the international destination. One option would be to use a local carrier in the destination country as the partner. A second option would be to use an Internet service provider, or some other service provider connected to the Internet in the destination country.

c) PSTN to PC

This case appears to be of least interest, although it has some application and is presented here for completeness.

As noted in the PC to PSTN case the PSTN to Internet gateway will need to support translating PCM to multiple encoding schemes to interwork with software from various vendors. The directory service is required to identify the called PC. Automatic notification of presence is important to keep the called party reachable. The PSTN caller need not be registered with the directory service, for caller billing will be based on PSTN information. The caller has an E.164 address that is "constant" and can be used to return calls as well as to do billing. Presumably we can deliver the calling number to the called party as an indication of who is calling. The calling number will not always be available, for technological or privacy reasons. It must be possible to signal the PC software that this is a PSTN call and provide the E.164 number or indicate that it is unavailable.

The service can be based on charging the calling phone. This can be done as if the Internet were the long distance portion of the call. This is possible

-180-

with a second dial tone. If an 800 or local dial service is used it is necessary for the caller to enter billing information. Alternatively a 900 service will allow PSTN caller-based billing. In either case the caller will need to specify the destination "phone number" after the billing information or after dialing
5 the 900 number.

A major open issue is how the caller will specify the destination at the second dial tone. Only touch tones are available at best. To simplify entry we could assign an E.164 address to each directory entry. To avoid
10 confusion with real phone numbers (the PSTN to PSTN case) the numbers need to be under directory control. Perhaps 700 numbers could be used, if there are enough available. Alternatively a special area code could be used. Spelling using the touch tone PAD is a less "user friendly" approach.

15 3. Phone Numbers in the Internet

The best approach is to have an area code assigned. Not only will this keep future options open, but it allows for simpler dialing from day one. Given a legitimate area code the PSTN caller can directly dial the E.164 address of the PC on the Internet. The telephone system will route the call to an MCI
20 POP where it will be further routed to a PSTN-to-Internet voice gateway. The called number will be used to place the call to the PC, assuming it is on-line and reachable. This allows the PSTN caller to dial the Internet as if it were part of the PSTN. No second dial tone is required and no billing information needs to be entered. The call will be billed to the calling PSTN station, and
25 charges will accrue only if the destination PC answers. Other carriers would be assigned unique area codes and directories should be kept compatible.

For domestically originated calls, all of the billing information needed to bill the caller is available and the intelligent network service functionality for
30 third party or other billing methods is available via the second dial tone.

-181-

4. Other Internet Telephony Carriers

All this will get more complicated when number portability becomes required. It may be desirable to assign a country code to the Internet. Although this would make domestic dialing more complex (it appears that
5 dialing anything other than 1 plus a ten digit number significantly reduces the use of the service) it may have some desirable benefits. In any event the assignment of an area code (or several) and the assignment of a country code are not mutually exclusive. The use of a country code would make dialing more geographically uniform.

10

5. International Access

It is unlikely that an international call will be made to the US to enter the Internet in the US. If it happens, however, the system will have enough information to do the caller-based billing for this case without any additional
15 functionality.

Another possibility is that we will (possibly in partnership) set up to handle incoming calls outside the US and enter the Internet in that country to return to the US, or go anywhere else on the Internet. If the partner is a
20 local carrier, then the partner will have the information needed for billing the PSTN caller.

a) Collect Calls

PSTN to PC collect calls require several steps. First, the call to the PSTN to
25 Internet gateway must be collect. The collect call could then be signaled in the same way as PC to PC calls. It will be necessary to indicate that the caller is PSTN based and include the calling E.164 address if it is available.

-182-

b) PSTN to PSTN

The choice of voice compression and protocol scheme for passing voice between PSTN to Internet gateways is entirely under the carrier's control.

5 Various service levels could be offered by varying the compression levels offered. Different charges could associated with each level. The caller would select a quality level; perhaps by dialing different 800 number services first.

(1) Domestic Destination

10 Neither the calling nor the called parties need be registered with the directory service to place calls across the Internet. The caller dials a PSTN-to-Internet gateway and receives a second dial tone and specifies, using touch tones, the billing information and the destination domestic E.164 address. 900 service could be used as well. The directory service (this could be separate system, but the directory service already has mapping

15 functionality to handle the PC to PSTN dial out case) will be used to map the call to an out dialer to place a local call, if possible. Billing is to the caller and the call detail of the out dial call needs to be associated with the call detail of the inbound caller.

20 An immediate question is how to deal with the case where the nearest dial out unit to the number called results in a long distance or toll call, as discussed in PC to PSTN case. The situation here is different to the extent that notification must be by voice, and authorization to do a long distance, or toll call dial out must be made by touch tones. In the event of a long

25 distance dial out the Internet could be skipped altogether and the call could go entirely over the PSTN. It is not clear that there is any cost savings by using the Internet in this case.

(2) One Step Dialing

30 The problem is that the destination PSTN number needs to be entered and,

-183-

somehow, it needs to be indicated that the destination is to be reached via the Internet rather than the conventional long distance network.

This selection criteria can be conveyed according to the following alternatives:

- 5 1. Assign a new 10XXX number that is the carrier's Internet.
2. By subscription.

The first method allows the caller to select the Internet as the long distance carrier on a call by call basis. The second method makes the Internet the default long distance network. In the second case a customer can return to
10 the carrier's conventional long distance network by dialing the carrier's 10XXX code.

The first method has the draw back that the caller must dial an extra five digits. Although many will do this to save money, requiring any extra
15 dialing will reduce the total number of users of the service. The second method avoids the need to dial extra digits, but requires a commitment by the subscriber to predominately use the Internet as his long distance network. The choice is a lower price with a lower quality of service.

20 In the PSTN to PSTN case it is possible to consider offering several grades of service at varying prices. These grades will be based on a combination of the encoding scheme and the amount of compression (bandwidth) applied, and will offer lower cost for lower bandwidth utilization.

25 To signal the grade of service desired three 10XXX codes could be used. By subscription a particular grade would be the default and other service grades would be selected by a 10XXX code.

(3) Service Quality

30 The service quality will be measured by two major factors. First, sound quality, the ability to recognize the caller's voice, and second by the delays

-184-

that are not present in the PSTN.

On the first point we can say that most of the offerings available today provide an acceptable level of caller recognition. Delay, however, is another story. PC to PC users experience delays of a half second to two seconds. As noted in the introduction much of the delay can be attributed to the sound cards and the low speed dial access. In the case of PSTN to PSTN service both these factors are removed.

- 10 The use of DSPs in the PSTN to Internet voice gateway will keep compression and protocol processing times very low. The access to the gateway will be at a full 64 kbps on the PSTN side and likely Ethernet on the Internet side. Gateways will typically be located close to the backbone so the router on the Ethernet will likely be connected to the backbone by a T3 line. This combination should provide a level of service with very low delays. Some buffering will be needed to mask the variable delays in the backbone, but that can likely be kept to under a quarter of a second in the domestic carrier backbone.
- 20 The main differentiation of quality of service will be voice recognition which will be related to bandwidth usage. If needed, the proposed IETF Resource reSerVation setup Protocol (RSVP) can be used to assure lower delay variation, but the need for the added complexity of RSVP is yet to be established. Also, questions remain regarding the scalability of RSVP for large-scale internet telephony.

(4) Costs

- An open question is whether using the Internet for long distance voice in place of the switched telephone network is actually cheaper. Certainly it is priced that way today, but do current prices reflect real costs? Routers are certainly cheaper than telephone switches, and the 10 kbps (or so) that the IP voice software uses (essentially half duplex) is certainly less than the

-185-

dedicated 128 kbps of a full duplex 64 kbps DS0. Despite these comparisons the question remains.

Although routers are much cheaper than telephone switches, they have
5 much less capacity. Building large networks with small building blocks gets
not only expensive, but quickly reaches points of diminishing returns. We
already have seen the Internet backbone get overloaded with the current
crop of high end routers, and they are yet to experience the significant traffic
increase that a successful Internet Telephony offering would bring. We are
10 saying two things here.

1. It is unlikely that the current Internet backbone can support a major
traffic increase associated with a successful internet telephony service. We
need to wait for the technology of routers to improve.

15

2. The second issue raised above was that of bandwidth usage. Indeed
10 kbps half duplex (a little more when both parties occasionally speak at
the same time, but much less during periods of silence) is considerably less
than 64 kbps full duplex dedicated capacity. Two points should be noted on
20 this argument.

First, bandwidth is cheap, at least, when there is spare fiber in the ground.
Once the last strand is used the next bit per second is very expensive.
Second, on transoceanic routes, where bandwidth is much more expensive,
25 we are already doing bandwidth compression of voice to 9.6 kbps. This is
essentially equivalent to the 10 kbps of Internet Telephony.

Why is IP capacity priced so much cheaper than POTS? The answer is that
the pricing difference is partly related to the subsidized history of the
30 Internet. There is a process in motion today, by the Internet backbone
providers, to address some of the cost issues of the Internet. The essence of
the process is the recognition that the Internet requires a usage charge.

-186-

Such charges already apply to some dial up users, but typically do not apply to users with dedicated connections.

5 If PC to PC Internet Telephony becomes popular, users will tend to keep their PCs connected for long periods. This will make them available to receive calls. It will also drive up hold times on dial in ports. This will have a significant effect on the capital and recurring costs of the Internet.

(5) Charges

10 A directory service must provide the functions described above and collect enough information to bill for the service. A charge can be made for directory service as well as for registration (a one time fee plus a monthly fee), call setup, but probably not for duration. Duration is already charged for the Internet dial in user and is somewhat bundled for the LAN-attached user.

15 Usage charges for Internet service may be coming soon (as discussed above). Duration charges are possible for the incoming and outgoing PSTN segments.

Incoming PSTN calls may be charged as the long distance segment by using
20 a special area code. Other direct billing options are 900 calls and calling card (or credit card) billing options (both require a second dial tone).

Requiring all callers (except incoming PSTN calls) to be registered with the directory service will eliminate the immediate need for most collect calling.

25 This will probably not be a great impediment since most users of the IP Phone service will want to receive as well as originate calls, and registration is required for receiving calls. Callers could have unlisted entries which would be entries with an E.164 address, but no name. People given this E.164 address could call the party (from the PSTN or from a PC), as is the

30 case in the present phone system.

-187-

Different compression levels can be used to provide different quality of voice reproduction and at the same time use more or less Internet transit resources. For PC to PC connections the software packages at both ends can negotiate the amount of bandwidth to be used. This negotiation might be facilitated through the directory service.

(6) Technical Issues

It will be necessary to coordinate with IP Phone vendors to implement the registration, automatic presence notification, and verification capabilities.

10 We will also need to add the ability to communicate service requests. These will include authorization for collect calls specifying attributes such as "place a dial out call to the PSTN even if it is long distance" and others to be determined.

15 Registration with a directory is a required feature that will be illuminated below. Using the DNS model for the distributed directory service will likely facilitate this future requirement. Assignment of a pseudo E.164 number to directory entries will work best if a real area code is used. If each carrier has an area code it will make interworking between the directory systems much easier. An obvious complication will arise when number portability becomes required.

IP Telephony, in accordance with a preferred embodiment, is here and will stay for at least the near future. A combination of a carrier level service, based on this technology, and a growth in the capacity of routers may lead to the Internet carrying a very significant percentage of future long distance traffic.

30 The availability of higher speed Internet access from homes, such as cable modems, will make good quality consumer IP Telephony service more easily attained. The addition of video will further advance the desirability of the

-188-

service.

More mundane, but of interest, is FAX services across the Internet. This is very similar to the voice service discussed above. Timing issues related to FAX protocols make this a more difficult offering in some ways.

Conferencing using digital bridges in the Internet make voice and video services even more attractive. This can be done by taking advantage of the multi-casting technology developed in the Internet world. With multi-casting the cost of providing such services will be reduced.

C. Internet Telephony Services

Figure **1C** is a block diagram of an internet telephony system in accordance with a preferred embodiment. Processing commences when telephone **200** is utilized to initiate a call by going off hook when a party dials a telephone number. Telephone **200** is typically connected via a conventional two-wire subscriber loop through which analog voice signals are conducted in both directions. One of ordinary skill in the art will readily realize that a phone can be connected via fiber, ISDN or other means without departing from the teaching of the invention. Alternatively, a person could dial a phone number from a computer **210**, paging system, video conferencing system or other telephony capable devices. The call enters a Local Exchange Carrier (LEC) **220** which is another name for a Regional Bell Operating Company (RBOC) central switch. The call is terminated by a LEC at a leased Common Business Line (CBL) **230** of an interchange carrier such as MCI. As a result of the termination to the CBL, the MCI Switch **221** receives an offhook indication.

The Switch **221** responds to the offhook by initiating a DAL Hotline procedure request to the Network Control System (NCS) which is also referred to as a Data Access Point (DAP) **240**. The switch **221** is simplified

-189-

to show it operating on a single DS1 line, but it will be understood that switching among many lines actually occurs so that calls on thousands of individual subscriber lines can be routed through the switch on their way to ultimate destinations. The DAP **240** returns a routing response to the
5 originating switch **221** which instructs the originating switch **221** to route the call to the destination switch **230** or **231**. The routing of the call is performed by the DAP **240** translating the transaction information into a specific SWitch ID (SWID) and a specific Terminating Trunk Group (TTG) that corresponds to the route out of the MCI network necessary to arrive at
10 the appropriate destination, in this case either switch **230** or **231**. An alternative embodiment of the hybrid network access incorporates the internet access facility into a switch **232**. This integrated solution allows the switch **232** to attach directly to the internet **295** which reduces the number of network ports necessary to connect the network to the internet **295**. The
15 DAP sends this response information to the originating switch **221** which routes the original call to the correct Terminating Switch **230** or **231**. The terminating switch **230** or **231** then finds the correct Terminating Trunk Group (TTG) as indicated in the original DAP response and routes the call to the ISN **250** or directly to the modem pool **270** based on the routing
20 information from the DAP **240**. If the call were destined for the Intelligent Services Network (ISN) **250**, the DAP **240** would instruct the switch to terminate at switch **230**.

Based upon analysis of the dialed digits, the ISN routes the call to an Audio
25 Response Unit (ARU) **252**. The ARU **252** differentiates voice, fax, and modem calls. If the call is from a modem, then the call is routed to a modem pool **271** for interfacing to an authentication server **291** to authenticate the user. If the call is authenticated, then the call is forwarded through the UDP/IP or TCP/IP LAN **281** or other media communication
30 network to the Basic Internet Protocol Platform (BIPP) **295** for further processing and ultimate delivery to a computer or other media capable device.

-190-

If the call is voice, then the ARU prompts the caller for a card number and a terminating number. The card number is validated using a card validation database. Assuming the card number is valid, then if the terminating
5 number is in the US (domestic), then the call would be routed over the current MCI voice lines as it is today. If the terminating number is international, then the call is routed to a CODEC **260** that converts the voice to TCP/IP or UDP/IP and sends it via the LAN **280** to the internet **295**.
The call is routed through a gateway at the terminating end and ultimately
10 to a phone or other telephony capable device.

Figure **1D** is a block diagram of a hybrid switch in accordance with a preferred embodiment. Reference numbers have been conserved from Figure **1C**, and an additional block **233** has been added. Block **233**
15 contains the connecting apparatus for attaching the switch directly to the internet or other communication means. The details of the connecting apparatus are presented in Figure **1E**. The principal difference between the hybrid switch of Figure **1D** and the switches presented in Figure **1C** is the capability of switch **221** attaching directly to the Internet **295**.

Figure **1E** is a block diagram of the connecting apparatus **233** illustrated in Figure **1D** in accordance with a preferred embodiment. A message bus **234** connects the switch fabric to an internal network **236** and **237**. The internal network in turn receives input from a Dynamic Telephony
25 Connection (DTC) **238** and **239** which in turn provides demuxing for signals originating from a plurality of DS1 lines **242**, **243**, **244** and **245**. DS1 lines, described previously, refer to the conventional bit format on the T1 lines.

To accommodate the rapidly diversifying telephony / media environment, a
30 preferred embodiment utilizes a separate switch connection for the other internal network **237**. A Spectrum Peripheral Module (SPM) **247** is utilized to handle telephony/media signals received from a pooled switch matrix

-191-

248, 249, 251, 254, 261-268. The pooled switch matrix is managed by the SPM **247** through switch commands through control lines. The SPM **247** is in communication with the service provider's call processing system which determines which of the lines require which type of hybrid switch

5 processing. For example, fax transmissions generate a tone which identifies the transmission as digital data rather than digitized voice. Upon detecting a digital data transmission, the call processing system directs the call circuitry to allow the particular input line to connect through the pooled switch matrix to a corresponding line with the appropriate processing
10 characteristics. Thus, for example, an internet connection would be connected to a TCP/IP Modem line **268** to assure proper processing of the signal before it was passed on through the internal network **237** through the message bus **234** to the originating switch **221** of Figure **1D**.

15 Besides facilitating direct connection of a switch to the internet, the pooled switch matrix also increases the flexibility of the switch for accommodating current communication protocols and future communication protocols. Echo cancellation means **261** is efficiently architected into the switch in a manner which permits echo cancellation on an as-needed basis. A relatively
20 small number of echo cancellers can effectively service a relatively large number of individual transmission lines. The pooled switch matrix can be configured to dynamically route either access-side transmissions or network-side transmissions to OC3 demux, DSP processing or other specialized processing emanating from either direction of the switch.

25

Moreover, a preferred embodiment as shown in Figure **1E** provides additional system efficiencies such as combining multiplexer stages in a port device on one side of a voice or data circuit switch to enable direct connection of a fiber-optic cable to the multiplexed output of the port device.

30 Moreover, redundancy is architected into the switch through the alternate routes available over CEM **248 / 249** and RM **251 / 254** to alternate paths for attaching various communication ports.

-192-

When the switch **221** of Figure **1D**, is connected to the internet **295**, the processing is provided as follows. A line from the internet **295** enters the switch through a modem port **268** and enters the pooled switch matrix
5 where demux and other necessary operations are performed before the information is passed to the switch **221** through the internal network **237** and the message bus **234**. The modules **261-268** provide plug and play capability for attaching peripherals from various communication disciplines.

10 Figure **1F** is a block diagram of a hybrid (internet-telephony) switch in accordance with a preferred embodiment. The hybrid switch **221** switches circuits on a public switched telephone network (PSTN) **256** with TCP/IP or UDP/IP ports on an internet network **295**. The hybrid switch **221** is composed of PSTN network interfaces (**247, 260**), high-speed Internet
15 network interfaces (**271, 272, 274**), a set of Digital Signal Processor (DSP)s (**259, 263**), a time-division multiplexed bus **262**, and a high-speed data bus **275**.

The hybrid internet telephony switch **221** grows out of the marriage of
20 router architectures with circuit switching architectures. A call arriving on the PSTN interface **257** is initiated using ISDN User Part (ISUP) signaling, with an Initial Address Message (IAM), containing a called party number and optional calling party number. The PSTN interface **257** transfers the IAM to the host processor **270**. The host processor **270** examines the PSTN
25 network interface of origin, the called party number and other IAM parameters, and selects an outgoing network interface for the call. The selection of the outgoing network interface is made on the basis of routing tables. The switch **221** may also query an external Service Control Point (SCP) **276** on the internet to request routing instructions. Routing
30 instructions, whether derived locally on the switch **221** or derived from the SCP **276**, may be defined in terms of a subnet to use to reach a particular destination.

-193-

Like a router, each of the network interfaces in the switch **221** is labeled with a subnet address. Internet Protocol (IP) addresses contain the subnet address on which the computer is located. PSTN addresses do not contain
5 IP subnet addresses, so subnets are mapped to PSTN area codes and exchanges. The switch **221** selects routes to IP addresses and PSTN addresses by selecting an interface to a subnet which will take the packets closer to the destination subnet or local switch.

10 The call can egress the switch via another PSTN interface **258**, or can egress the switch via a high-speed internet network interface **273**. If the call egresses the switch via the PSTN interface **258**, the call can egress as a standard PCM Audio call, or can egress the switch as a modem call carrying compressed digital audio.

15

In the case where the call egresses the switch **221** as a standard PCM audio call, the PCM audio is switched from PSTN Interface **257** to PSTN Interface **258** using the TDM bus **260**. Similarly, PCM audio is switched from PSTN Interface **258** to PSTN Interface **257** using the TDM bus **260**.

20

In the case where the call egresses the switch **221** as a modem call carrying compressed digital audio, the switch **221** can initiate an outbound call to a PSTN number through a PSTN interface **258**, and attach across the TDM Bus **260** a DSP resource **259** acting as a modem. Once a modem session is
25 established with the destination, the incoming PCM audio on PSTN interface **257** can be attached to a DSP Resource **263** acting as an audio codec to compress the audio. Example audio formats include ITU G.729 and G.723. The compressed audio is packetized into Point to Point Protocol (PPP) packets on the DSP **263**, and transferred to DSP **259** for modem delivery
30 over the PSTN Interface **258**.

In the case where the call egresses the switch **221** on a high speed internet

-194-

interface **272**, the switch **221** attaches the PSTN Interface **257** to the DSP resource **263** acting as an audio codec to compress the PCM audio, and packetize the audio into UDP/IP packets for transmission over the Internet network. The UDP/IP packets are transferred from the DSP resource **263** over the high-speed data bus **275** to the high-speed internet network interface **272**.

Figure **1G** is a block diagram showing the software processes involved in the hybrid internet telephony switch **221**. Packets received on the internet network interface **296** are transferred to the packet classifier **293**. The packet classifier **293** determines whether the packet is a normal IP packet, or is part of a routing protocol (ARP, RARP, RIP, OSPF, BGP, CIDR) or management protocol (ICMP). Routing and management protocol packets are handed off to the Routing Daemon **294**. The Routing Daemon **294** maintains routing tables for the use of the packet classifier **293** and packet scheduler **298**. Packets classified as normal IP packets are transferred either to the packetizer/depacketizer **292** or to the packet scheduler **298**. Packets to be converted to PCM audio are transferred to the packetizer/depacketizer **292**. The packetizer/depacketizer takes packet contents and hands them to the codec **291**, which converts compressed audio into PCM Audio, then transfers PCM audio to the PSTN Interface **290**.

Normal IP packets to be sent to other internet devices are handed by the packet classifier **293** to the packet scheduler **298**, which selects the outgoing network interface for the packet based on the routing tables. The packets are placed upon an outbound packet queue for the selected outgoing network interface, and the packets are transferred to the high speed network interface **296** for deliver across the internet **295**.

D. Call Processing

This section describes how calls are processed in the context of the networks

-195-

described above.

1. VNET Call Processing

Figure **10A** illustrates a Public Switched Network (PSTN) **1000** comprising a local exchange (LEC) **1020** through which a calling party uses a telephone **1021** or computer **1030** to gain access to a switched network including a plurality of MCI switches **1011**, **1010**. Directory services for routing telephone calls and other information is provided by the directory services **1031** which is shared between the Public Branch Exchanges **1041**, **1040** and the PSTN.

10 This set of scenarios allows a subscriber to use either a PC, telephone or both to make or receive VNET calls. In this service, the subscriber may have the following equipment:

- A telephone that uses VNET routing is available today in MCI's network. In this case, VNET calls arriving in the MCI PSTN network using the subscriber's VNET number are routed with the assistance of the DAP just as they are routed today.
- A PC that is capable of Internet telephony. Calls are routed into and out of this PC with the assistance of an Internet or Intranet Directory Service that tracks the logged-in status and current IP address of the VNET user.
- 20 • A PC and a telephone is used to receive and make calls. In this case, a user profile will contain information that allows the DAP and Directory Service to make a determination whether to send an incoming call to the PC or to the telephone. For example, the user may always want calls to go to their PC when they are logged-in and to their phone at all other times. Or, 25 they may want their calls to always go to their PC during normal work hours and to their phone at other times. This type of control over the decision to send incoming calls to a phone or PC may be controlled by the subscriber.

The following scenarios apply to this type of service.

-196-

1. A PC to PC call where the Directory service is queried for the location of the terminating PC:

- PCs connected to an Intranet using the Intranet as transport.
- Both PC's connected to a corporate Intranet via dial up access.
- Both PCs on separate Intranets with the connection made through the Internet.
- Both PCs on the Internet through a dial-up connection.
- One PC directly connected to a corporate Intranet and the other PC using a dial-up connection to the Internet.
- One PC using a dial up connection to a corporate Intranet and the other PC using a dial-up connection to the Internet.
- Both PCs on separate Intranets with the connection made through the PSTN.
- One or both PCs connected to a corporate Intranet using dial-up access.
- One or both of the PCs connected to an Internet Service Provider.
- One or both of the ITGs as an in-network element.

2. A PC to phone call where a directory service is queried to determine that the terminating VNET is a phone. The PC then contacts an Internet

5 Telephony Gateway to place a call to the terminating phone.

- PC on an intranet using a private ITG connected to the PSTN with the ITG as an out of network element. The destination phone is connected to a PBX.
- The PC may also be using a public ITG that must be access through the Internet.

10 • The PC may be connected to the corporate Intranet using dial-up access.

- PC on an intranet using a private ITG connected to the PSTN with the ITG as an in-network element. The destination phone is connected to a PBX.

-197-

- The PC may also be using a public ITG that must be accessed through the Internet.
- The PC may be connected to the corporate Intranet using dial-up access.
- PC on an intranet using a private ITG connected to the PSTN with the ITG as an in-network element. The destination phone is connected to the PSTN.
- The PC may also be using a public ITG that must be accessed through the Internet.
- The PC may be connected to the corporate Intranet using dial-up access.
- The ITG may be an in-network element.
- PC on an intranet using a private ITG connected to a PBX with the traffic carried over the Intranet.
- PC is at a different site than the destination phone with the traffic carried over the Internet or intranet.
- The PC may be using a dial-up connection to the corporate Intranet.

15

3. A phone to PC call where the DAP or PBX triggers out to the Internet Directory Service to identify the terminating IP address and ITG for routing the call. The call is then routed through the PSTN to an ITG and a connection is made from the ITG to the destination PC.

20 Possible Variations:

Same variations as the PC to phone.

4. A Phone to Phone call where the DAP or PBX must query the Directory Service to determine whether the call should be terminated to the subscriber's phone or PC.

25

Possible Variations:

- Both Phones are on a PBX;

-198-

- One phone is on a PBX and the other phone is on the PSTN; and
- Both phones are on the PSTN.

5 For each of these variations, the DAP and Directory Service may be a single entity or they may be separate entities. Also, the directory service may be a private service or it may be a shared service. Each of the scenarios will be discussed below with reference to a call flow description in accordance with a preferred embodiment. A description of the block elements associated with each of the call flow diagrams is presented below to assist in understanding the embodiments.

10 2. Descriptions of Block Elements

Element	Description
Ph1	<p>Traditional analog phone connected to a Local Exchange Carrier. For the purposes of these VNET scenarios, the phone is capable of making VNET calls, local calls or DDD calls. In some scenarios the VNET access may be done through</p> <ul style="list-style-type: none"> • The customer dials a 700 number with the last seven digits being the destination VNET number for the call. The LEC will know that the phone is picked to MCI and route the call to the MCI switch. The MCI switch will strip off the "700", perform an ANI lookup to identify the customer ID and perform VNET routing using the VNET number and customer ID. • The customer dials an 800 number and is prompted to enter their Social Security number (<i>or other unique id</i>) and a VNET number. The switch passes this information to the DAP which does the VNET translation.
PC1 PC2	Personal computer that has the capability to dial in to an Internet service provider or a corporate intranet for the purpose of making

	<p>or receiving Internet telephony calls. The following access methods might be used for this PC</p> <p>Internet service provider</p> <ul style="list-style-type: none"> • The PC dials an 800 number (<i>or any other dial plan</i>) associated with the service provider and is routed via normal routing to the modem bank for that provider. The user of the PC then follows normal log-on procedures to connect to the Internet. <p>Corporate Intranet</p> <ul style="list-style-type: none"> • The PC dials an 800 number (<i>or any other dial plan</i>) associated with the corporate Intranet and is routed via normal routing to the modem bank for that Intranet. The user of the PC then follows normal log-on procedures to connect to the Intranet.
LEC SF1	Switching fabric for a local exchange carrier. This fabric provides the connection between Ph1/PC1/PC2 and MCI's telephone network. It also provides local access to customer PBXs.
MCI SF1 MCI SF2	Switching fabric for MCI (or for the purpose of patenting, any telephony service provider). These SFs are capable of performing traditional switching capabilities for MCI's network. They are able to make use of advanced routing capabilities such as those found in MCI's NCS (Network Control System).
NCS	The NCS provides enhanced routing services for MCI. Some of the products that are supported on this platform are: 800, EVS, Universal Freephone, Plus Freephone, Inbound International, SAC(ISAC) Codes, Paid 800, 8XX/Vnet Meet Me Conference Call, 900, 700, PCS, Vnet, Remote Access to Vnet, Vnet Phone Home, CVNS, Vnet Card, MCI Card (950 Cards), Credit Card and GETS Card.

-200-

	<p>In support of the existing VNET services, the DAP provides private dialing plan capabilities to Vnet customers to give them a virtual private network. The DAP supports digit translation, origination screening, supplemental code screening, 800 remote access, and some special features such as network call redirect for this service.</p> <p>To support the call scenarios in this document, the NCS also has the capability to made a data query to directory services in order to route calls to PCs.</p>
Dir Svc 1	Internet Directory Services. The directory service performs:
Dir Svc 2	<ul style="list-style-type: none"> • Call routing - As calls are made to subscribers using Internet telephony services from MCI, the directory service must be queried to determine where the call should terminate. This may be done based upon factors such as <ul style="list-style-type: none"> – the logged-in status of the subscriber, – service subscriptions identifying the subscriber as a PC or phone only user – preferred routing choices such as “route to my PC always if I am logged in”, or “route to my PC from 8-5 on weekdays, phone all other times”, etc. • Customer profile management - The directory service must maintain a profile for each subscriber to be able to match VNET numbers to the service subscription and current state of subscribers. • Service authorization - As subscribers connect their PCs to an IP telephony service, they must be authorized for use of the service and may be given security tokens or encryption keys to ensure access to the service. This authorization responsibility might also place restrictions upon the types of service a user might be able to access, or introduce range privileges restricting

-201-

	the ability of the subscriber to place certain types of calls.
ITG 1 ITG 2	<p>Internet Telephony Gateway - The Internet Telephony Gateway provides a path through which voice calls made be bridged between an IP network and a traditional telephone network.</p> <p>To make voice calls from an IP network to the PSTN, a PC software package is used to establish a connection with the ITG and request that the ITG dial out on the PSTN on behalf of the PC user. Once the ITG makes the connection through the voice network to the destination number, the ITG provides services to convert the IP packetized voice from the PC to voice over the PSTN. Similarly, the ITG will take the voice from the PSTN and convert it to IP packetized voice for the PC.</p> <p>To make voice calls from the PSTN to the IP network, a call will be routed to the ITG via PSTN routing mechanisms. Once the call arrives, the ITG identifies the IP address for the destination of the call, and establishes an IP telephony session with that destination. Once the connection has been established, the ITG provides conversion services between IP packetized voice and PCM voice.</p>
ITG 3 ITG 4	These ITGs act in a similar capacity as the ITGs connected to the PSTN, but these ITGs also provide a connection between the corporate Intranet and the PBX.
IAD 1 IAD 2	The Internet access device provides general dial-up Internet access from a user's PC to the Internet. This method of connecting to the Internet may be used for Internet telephony, but it may also be simply used for Internet access. When this device is used for Internet telephony, it behaves differently than the ITG. Although the IAD is connected to the PSTN, the information traveling over that interface is not PCM voice, it is IP data packets. In the case of telephony over the IAD, the IP data packets happen to be voice packets, but the IAD has no visibility into those packets and

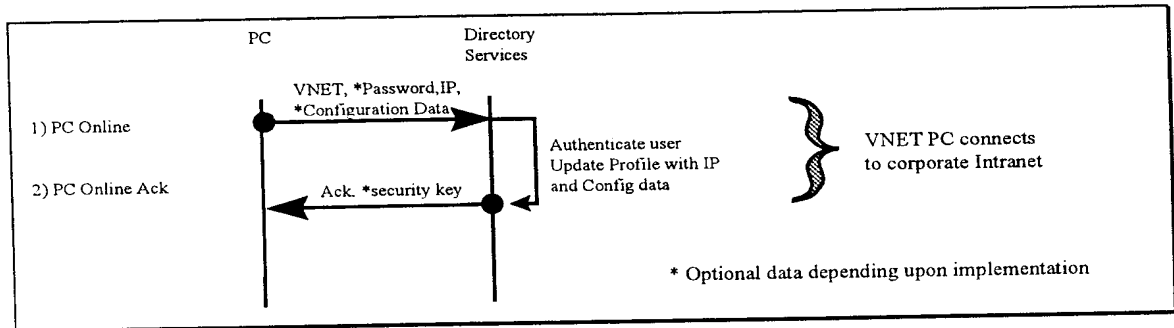
-202-

	cannot distinguish a voice packet from a data packet. The IAD can be thought of as a modem pool that provides access to the Internet.
PBX 1 PBX 2	<p>Private Branch Exchange - This is customer premise equipment that provides connection between phones that are geographically co-located. The PBX also provides a method from those phones to make outgoing calls from the site onto the PSTN. Most PBXs have connections to the LEC for local calls, and a DAL connection to another service provider for VNET type calls.</p> <p>These PBXs also show a connection to a Directory Service for assistance with call routing. This capability does not exist in today's PBXs, but in the VNET call flows for this document, a possible interaction between the PBX and the Directory Service is shown.</p> <p>These PBXs also show a connection to an ITG. These ITGs provide the bridging service between a customer's Intranet and the traditional voice capabilities of the PBX.</p>
Ph11 Ph12 Ph21 Ph22	These are traditional PBX connected phones.
PC 11 PC12 PC21 PC22	These are customer premises PCs that are connected to customer Intranets. For the purposes of these call flows, the PCs have Internet Telephony software that allow the user to make or receive calls.

-203-

E. Re-usable Call Flow Blocks

1. VNET PC connects to a corporate intranet and logs in to a directory service



1. The user for a PC connects their computer to an IP network, turns on the computer and starts an IP telephony software package. The software package sends a message to a directory service to register the computer as "on-line" and available to receive calls. This on-line registration message would most likely be sent to the directory service in an encrypted format for security. The encryption would be based upon a common key shared between the PC and the directory service. This message contains the following information:
 - Some sort of identification of the computer or virtual private network number that may be used to address this computer. In this VNET scenario, this is the VNET number assigned to the individual using this PC. This information will be used to identify the customer profile associated with this user. *It may also be some identification such as name, employee id, or any unique ID which the directory service can associate with a VNET customer profile.*
 - A password or some other mechanism for authenticating the user identified by the VNET number.

-204-

- The IP address identifying the port that is being used to connect this computer to the network. This address will be used by other IP telephony software packages to establish a connection to this computer.
- The message may contain additional information about the specifics of the software package or PC being used for IP telephony and the configuration/capabilities of the software or PC. As an example it might be important for a calling PC to know what type of compression algorithms are being used, or other capabilities of the software or hardware that might affect the ability of other users to connect to them or use special features during a connection.

The location of the directory service to receive this "on-line" message will be determined by the data distribution implementation for this customer. In some cases this may be a private database for a company or organization subscribing to a VNET service, in other cases it might be a national or worldwide database for all customers of a service provider (MCI). This location is configured in the telephony software package running on the PC.

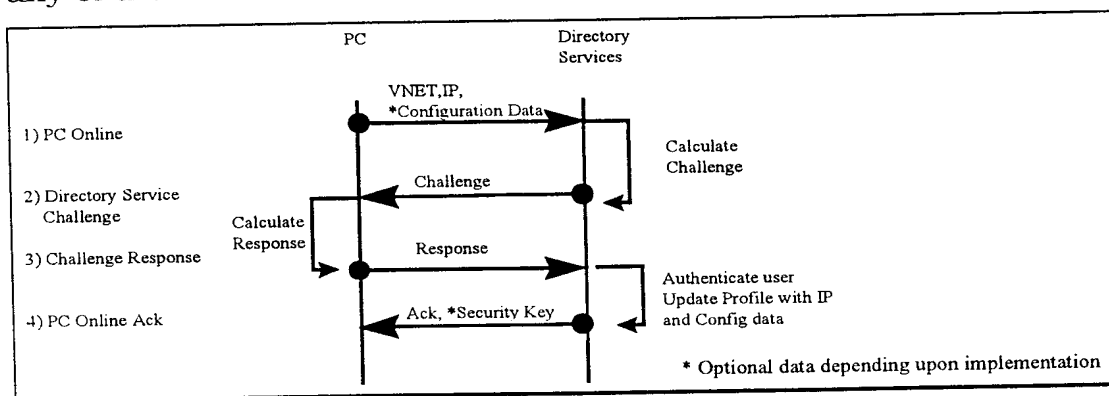
2. When the directory service receives this message from the PC, it validates the user by using the VNET number to look up a user profile and comparing the password in the profile to the password received. Once the user has been validated, the directory service will update the profile entry associated with the VNET number (*or other unique ID*) to indicate that the user is "on-line" and is located at the specified IP address. The directory service will also update the profile with the configuration data sent during the login request. Upon successful update of the, the directory service sends a response back to the specified IP address indicating that the message was received and processed. This acknowledgment

-205-

message may also contain some sort of security or encryption key to guarantee secure communication with the directory service when issuing additional commands. When the PC receives this response message it may choose to notify the user via a visual or audible indicator.

Variation for On-line registration

The call flow segment shown earlier in this section showed a PC on-line registration where the PC simply sends a password to the directory service to log-on. A variation for this log-on procedure would be the following call flow segment where the directory service presents a challenge and the PC user must respond to the challenge to complete the log-in sequence. This variation on the log-in sequence is not shown in any of the call flows contained within this document, but it could be used in any of them.



1. The user for a PC connects their computer to an IP network, turns on the computer and starts an IP telephony software package. The software package sends a message to a directory service to register the computer as "on-line" and available to receive calls. This on-line registration message would most likely be sent to the directory service in an encrypted format for security. The encryption would be based upon a common key shared between the PC and the directory service. This message contains the following information:
 - Some sort of identification of the computer or virtual private network number that may be used to address this computer.

-206-

In this VNET scenario, this is the VNET number assigned to the individual using this PC. This information will be used to identify the customer profile associated with this user. *It may also be some identification such as name, employee id, or any unique ID which the directory service can associate with a VNET customer profile.*

- The IP address identifying the port that is being used to connect this computer to the network. This address will be used by other IP telephony software packages to establish a connection to this computer.
- The message may contain additional information about the specifics of the software package or PC being used for IP telephony and the configuration/capabilities of the software or PC. As an example it might be important for a calling PC to know what type of compression algorithms are being used, or other capabilities of the software or hardware that might affect the ability of other users to connect to them or use special features during a connection.

The location of the directory service to receive this "on-line" message will be determined by the data distribution.

implementation for this customer. In some cases this may be a private database for a company or organization subscribing to a VNET service, in other cases it might be a national or worldwide database for all customers of a service provider (MCI). This location is configured in the telephony software package running on the PC.

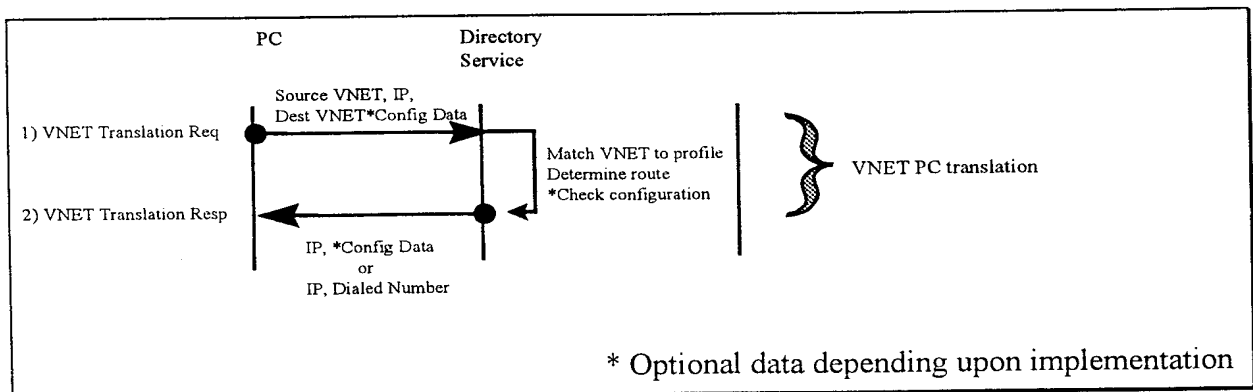
2. In this scenario the PC did not provide a password in the initial registration message. This is because the directory service uses a challenge/response registration process. In this case, the directory service will use a shared key to calculate a challenge that will be presented to the PC

-207-

3. The PC receives this challenge and presents it to the user of the PC. The PC user uses the shared key to calculate a response to the challenge and send the response back to the directory service.

4. When the directory service receives this response from the PC, it validates the user. Once the user has been validated, the directory service will update the profile entry associated with the VNET number (*or other unique ID*) to indicate that the user is "on-line" and is located at the specified IP address. The directory service will also update the profile with the configuration data sent during the login request. Upon successful update of the, the directory service sends a response back to the specified IP address indicating that the message was received and processed. This acknowledgment message may also contain some sort of security or encryption key to guarantee secure communication with the directory service when issuing additional commands. When the PC receives this response message it may choose to notify the user via a visual or audible indicator.

2. VNET PC queries a directory service for a VNET translation



-208-

1. A PC uses an Internet telephony software package to attempt to connect to a VNET number. To establish this connection, the user of the PC dials the VNET number (*or other unique ID such as name, employee ID, etc*). Once the telephony software package has identified this call as a VNET type call, it will send a translation request to the directory service. At a minimum, this translation request will contain the following information:

- The IP address of the computer sending this request
- The VNET number of the PC sending this request.
- The Vnet number (*or other ID*) of the computer to be dialed.
- A requested configuration for the connection. For example, the calling PC might want to use white-board capabilities within the telephony software package and may wish to verify this capability on the destination PC before establishing a connection. If the VNET number does not translate to a PC, this configuration information may not provide any benefit, but at the time of sending this request the user does not know whether the VNET number will translate to a PC or phone.

2. When the directory service receives this message, it uses the Vnet number (*or other ID*) to determine if the user associated with that VNET number (*or other ID*) is "on-line" and to identify the IP address of the location where the computer may be contacted. This directory service may also contain and make use of features like time of day routing, day of week routing, ANI screening, etc.

If the VNET number translates into a PC that is "on-line", the directory service will compare the configuration information in this request to the configuration information available in the profile for the destination PC.

When the directory service returns the response to the translation request from the originating PC, the response will include

- The registered "on-line" IP address of the destination PC. This is the IP address that the originating PC may use to contact the destination PC

-209-

- Configuration information indicating the capabilities of the destination PC and maybe some information about which capabilities are compatible between the origination and destination PC.

5

If the VNET number translates to a number that must be dialed through the PSTN, the response message to the PC will contain the following

10

- An IP address of an Internet Telephony gateway that may be used to get this call onto MCI's PSTN. The selection of this gateway may be based upon a number of selection algorithms. This association between the caller and the ITG to be used is made based upon information in the profile contained within the directory service.
- A VNET number to be dialed by the ITG to contact the destination phone. In the case of this call flow this is the VNET number of the destination phone. This allows the call to use the existing VNET translation and routing mechanisms provided by the DAP.

15

If the VNET number translates to a phone which is reachable through a private ITG connected to the customer's PBX, the directory service will return the following.

20

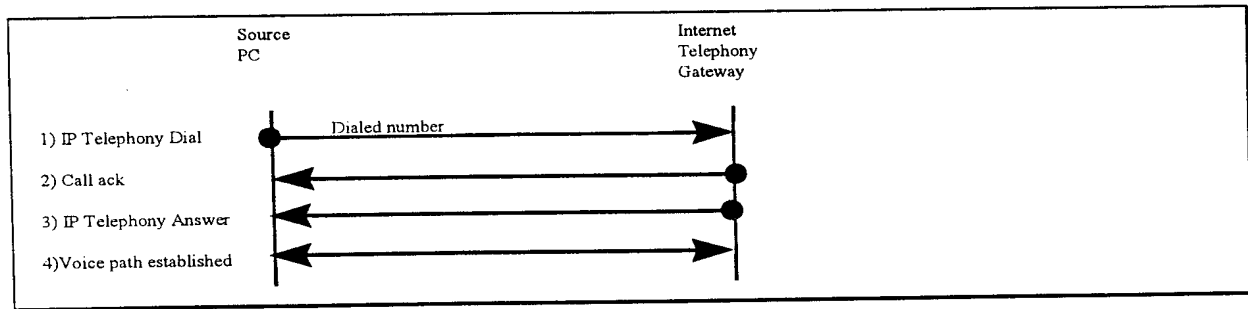
- The VNET number of an ITG gateway that is connected to the PBX serving the destination phone. This association between the destination phone the ITG connected to its serving PBX is made by the directory service.
- The VNET number to be dialed by the ITG when it offers the call to the PBX. In most cases this will just be an extension number.

25

30

3. PC connects to an ITG

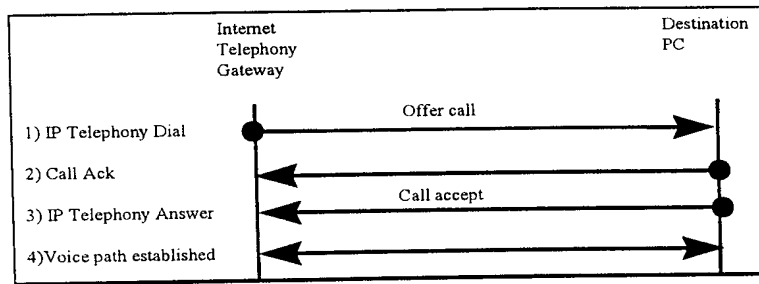
-210-



1. A PC uses its telephony software package to send a "connection" message to an ITG. This IP address is usually returned from the directory service in response to a VNET translation. The specific format and contents of this message is dependent upon the software sending the message or the ITG software to receive the message. This message may contain information identifying the user of the PC or it may contain information specifying the parameters associated with the requested connection.
2. The ITG responds to the connect message by responding to the message with an acknowledgment that a call has been received. This step of call setup may not be necessary for a PC calling an ITG, but it is shown here in an attempt to maintain a consistent call setup procedure that is independent of whether the PC is connecting to an ITG or to another PC. When connecting to a PC, this step of the procedure allows the calling PC to know that the destination PC is ringing.
3. The ITG accepts the call.
4. A voice path is established between the ITG and the PC.

4. ITG connects to a PC

-211-



1. An ITG uses its telephony software to send a "connection" message to a PC. The ITG must know the IP address of the PC to which it is connecting. The specific format and contents of this message is dependent upon the ITG software sending the message or the PC software to receive the message. This message may contain information identifying this call as one being offered from an ITG, or it may contain information specifying the requested configuration for the call (i.e. voice only call).
2. The message from step 1 is received by the PC and the receipt of this message is acknowledged by sending a message back to the ITG indicating that the PC is offering the call to the user of the PC
3. The user of the PC answers to call and a message is sent back to the originating PC indicating that the call has been accepted.
4. A voice path is established between the ITG and the PC.

5. VNET PC to PC Call Flow Description

The user for PC12 **1051** connects the computer to an Internet Protocol (IP) network **1071**, turns on the computer and starts an IP telephony software protocol system. The system software transmits a message to a directory service **1031** to register the computer as "on-line" and available to receive calls. This message contains IP address identifying the connection that is being used to connect this computer to the network. This address may be used by other IP telephony software packages to establish a connection to this computer. The address comprises an identification of the computer or

-212-

virtual private network number that may be used to address this computer **1051**. In this VNET scenario, the address is a VNET number assigned to the individual using this PC. VNET refers to a virtual network in which a particular set of telephone numbers is supported as a private network of numbers that can exchange calls. Many corporations currently buy communication time on a trunk that is utilized as a private communication channel for placing and receiving inter-company calls. The address may also be some identification such as name, employee id, or any other unique ID.

The message may contain additional information regarding the specifics of the system software or the hardware configuration of PC **1051** utilized for IP telephony. As an example, it is important for a calling PC to know what type of compression algorithms are supported and active in the current communication, or other capabilities of the software or hardware that might affect the ability of other users to connect or use special feature during a connection.

6. Determining best choice for Internet client selection of an Internet Telephony Gateway server on the Internet:

Figure **10B** illustrates an internet routing network in accordance with a preferred embodiment. If a client computer **1080** on the Internet needs to connect to an Internet Telephony Gateway **1084**, the ideal choice for an Gateway to select can fall into two categories, depending on the needs of the client:

If the client **1080** needs to place a telephone call to a regular PSTN phone, and PSTN network usage is determined to be less expensive or higher quality than Internet network usage, it is the preferred choice to select a gateway that allows the client to access the PSTN network from a point "closest" to the point of internet access. This is often referred to as Head-End Hop-Off

-213-

(HEHO), where the client hops off the internet at the "head end" or "near end" of the internet.

5 If the client **1080** needs to place a telephone call to a regular PSTN phone, and the PSTN network is determined to be more expensive than Internet network usage, it is the preferred choice to select a gateway that allows the client to access the PSTN from the Internet at a point closest to the destination telephone. This is often referred to as Tail-End Hop-Off (TEHO), where the client hops off the internet at the "tail end" or "far end" of the
10 internet.

a) Head-End Hop-Off Methods

(1) Client Ping Method

This method selects the best choice for a head-end hop-off internet telephony gateway by obtaining a list of candidate internet telephony gateway addresses, and pinging each to determine the best choice in terms
15 of latency and number of router hops. The process is as follows:

- Client Computer **1080** queries a directory service **1082** to obtain a list of candidate internet telephony gateways.
- The directory service **1082** looks in a database of gateways and selects a
20 list of gateways to offer the client as candidates. Criteria for selecting gateways as candidates can include
 - last gateway selected.
 - matching 1, 2, or 3 octets in the IPv4 address.
 - last client access point, if known.
 - 25 ■ selection of at least one gateway from all major gateway sites, if practical.
- The directory service **1082** returns a list of "n" candidate IP addresses to the client **1080** in a TCP/IP message.
- The client **1080** simultaneously uses the IP ping to send an echo-type message to each candidate Internet Telephony Gateway, **1084**, **1081**, **1086**.
- 30 The "-r" option will be used with the ping command to obtain a trace route.

-214-

■ Based upon the ping results for each Internet Telephony Gateway, the client **1080** will rank order the ping results as follows:

■ If any Internet Telephony Gateways are accessible to the client **1080** without traveling through any intervening router as revealed by the ping trace route, they are ranked first.

■ The remaining Internet Telephony Gateways are ranked in order of lowest latency of round-trip ping results.

Using the Client Ping Method with the Sample Network Topology above, the Client Computer **1080** queries the Directory Service **1082** for a list of Internet Telephony Gateways to ping. The Directory Service **1082** returns the list:

166.37.61.117

166.25.27.101

166.37.27.205

The Client Computer **1080** issues the following three commands simultaneously:

ping 166.37.61.117 -r 1

ping 166.25.27.101 -r 1

ping 166.37.27.205 -r 1

The results of the ping commands are as follows:

Pinging 166.37.61.117 with 32 bytes of data:

Reply from 166.37.61.117: bytes=32 time=3ms TTL=30

Route: 166.37.61.101

Reply from 166.37.61.117: bytes=32 time=2ms TTL=30

Route: 166.37.61.101

-215-

Reply from 166.37.61.117: bytes=32 time=2ms TTL=31

Route: 166.37.61.101

Reply from 166.37.61.117: bytes=32 time=2ms TTL=30

Route: 166.37.61.101

5

Pinging 166.25.27.101 with 32 bytes of data:

Reply from 166.25.27.101: bytes=32 time=14ms TTL=30

10 Route: 166.37.61.101

Reply from 166.25.27.101: bytes=32 time=2ms TTL=30

Route: 166.37.61.101

Reply from 166.25.27.101: bytes=32 time=3ms TTL=31

Route: 166.37.61.101

15 Reply from 166.25.27.101: bytes=32 time=4ms TTL=30

Route: 166.37.61.101

Pinging 166.37.27.205 with 32 bytes of data:

20

Reply from 166.37.27.205: bytes=32 time=1ms TTL=126

Route: 166.37.27.205

Reply from 166.37.27.205: bytes=32 time=1ms TTL=126

Route: 166.37. 27.205

25 Reply from 166.37. 27.205: bytes=32 time=1ms TTL=126

Route: 166.37. 27.205

Reply from 166.37. 27.205: bytes=32 time=1ms TTL=126

Route: 166.37. 27.205

30

Since the route taken to 166.37.27.205 went through no routers (route and ping addresses are the same), this address is ranked first. The remaining

-216-

Internet Telephony Gateway Addresses are ranked by order of averaged latency. The resulting preferential ranking of Internet Telephony Gateway addresses is

5 166.37.27.205
 166.37.61.117
 166.25.27.101

10 The first choice gateway is the gateway most likely to give high quality of service, since it is located on the same local area network. This gateway will be the first the client will attempt to use.

(2) Access Device Location Method

15 The method for identifying the most appropriate choice for an Internet Telephony Gateway utilizes a combination of the Client Ping Method detailed above, and the knowledge of the location from which the Client Computer **1080** accessed the Internet. This method may work well for clients accessing the Internet via a dial-up access device.

20 A client computer **1080** dials the Internet Access Device. The Access Device answers the call and plays modem tone. Then, the client computer and the access device establishes a PPP session. The user on the Client Computer is authenticated (username/password prompt, validated by an authentication server). Once the user passes authentication, the Access Device can automatically update the User Profile in the Directory Service for the
25 user who was authenticated, depositing the following information

 "User Name" "Account Code" "online timestamp"
 "Access Device Site Code"

30 Later, when the Client Computer requires access through an Internet Telephony Gateway, it queries the Directory Service **1082** to determine the best choice of Internet Telephony Gateway. If an Access Device Site Code is

-217-

found in the User's Profile on the Directory Service, the Directory Service **1082** selects the Internet Telephony Gateway **1084**, **1081** and **1086** at the same site code, and returns the IP address to the Client Computer **1080**. If an Internet Telephony Gateway **1084**, **1081** and **1086** is unavailable at the same site as the Access Device Site Code, then the next best choice is selected according to a network topology map kept on the directory server.

If no Access Device Site Code is found on the directory server **1082**, then the client **1080** has accessed the network through a device which cannot update the directory server **1082**. If this is the case, the Client Ping Method described above is used to locate the best alternative internet telephony gateway **1084**.

(3) User Profile Method

Another method for selection of an Internet Telephony Gateway **1084**, **1081** and **1086** is to embed the information needed to select a gateway in the user profile as stored on a directory server. To use this method, the user must execute an internet telephony software package on the client computer. The first time the package is executed, registration information is gathered from the user, including name, email address, IP Address (for fixed location computers), site code, account code, usual internet access point, and other relevant information. Once this information is entered by the user, the software package deposits the information on a directory server, within the user's profile.

25

Whenever the Internet Telephony software package is started by the user, the IP address of the user is automatically updated at the directory service. This is known as automated presence notification. Later, when the user needs an Internet Telephony Gateway service, the user queries the directory service for an Internet Telephony Gateway to use. The directory service knows the IP address of the user and the user's usual site and access point

30

-218-

into the network. The directory service can use this information, plus the network map of all Internet Telephony Gateways **1084**, **1081** and **1086**, to select the best Internet Telephony Gateway for the client computer to use.

(4) Gateway Ping Method

- 5 The last method selects the best choice for a head-end hop-off internet telephony gateway by obtaining a list of candidate internet telephony gateway addresses, and pinging each to determine the best choice in terms of latency and number of router hops. The process is as follows:
- 10 ■ Client Computer queries a directory service to obtain a best-choice internet telephony gateway.
 - The directory service looks in a database of gateways and selects a list of candidate gateways. Criteria for selecting gateways as candidates can include
 - 15 ■ last gateway selected.
 - matching 1, 2, or 3 octets in the IPv4 address.
 - last client access point, if known.
 - selection of at least one gateway from all major gateway sites, if practical.
 - 20 ■ The directory sends a message to each candidate gateway, instructing each candidate gateway to ping the client computer's IP Address.
 - Each candidate gateway simultaneously uses the IP ping to send an echo-type message to the client computer. The "-r" option will be used with the ping command to obtain a trace route. The ping results are returned from each candidate gateway to the directory service.
 - 25 ■ Based upon the ping results for each Internet Telephony Gateway, the directory service will rank order the ping results as follows:
 - If any Internet Telephony Gateways are accessible to the client without traveling through any intervening router as revealed by the ping trace route, they are ranked first.
 - 30 ■ The remaining Internet Telephony Gateways are ranked in order of lowest averaged latency of round-trip ping results.

-219-

The Client Ping Method and Gateway Ping Method may use the traceroute program as an alternative to the ping program in determining best choice for a head-end hop-off gateway.

b) Tail-End Hop-Off Methods

- 5 Tail-End Hop-Off entails selecting a gateway as an egress point from the internet where the egress point is closest to the terminating PSTN location as possible. This is usually desired to avoid higher PSTN calling rates. The internet can be used to bring the packetized voice to the local calling area of the destination telephone number, where lower local rates can be paid to
- 10 carry the call on the PSTN.

(1) Gateway Registration

- One method for Tail-End Hop-Off service is to have Internet Telephony Gateways **1084**, **1081** and **1086** register with a directory service. Each
- 15 Internet Telephony Gateway will have a profile in the directory service which lists the calling areas it serves. These can be listed in terms of Country Code, Area Code, Exchange, City Code, Line Code, Wireless Cell, LATA, or any other method which can be used to subset a numbering plan. The gateway, upon startup, sends a TCP/IP registration message to the Directory
- 20 Service **1082** to list the areas it serves.

- When a Client Computer wishes to use a TEHO service, it queries the directory service for an Internet Telephony Gateway **1084** serving the desired destination phone number. The directory service **1082** looks for a
- 25 qualifying Internet Telephony Gateway, and if it finds one, returns the IP address of the gateway to use. Load-balancing algorithms can be used to balance traffic across multiple Internet Telephony Gateways **1084**, **1081** and **1086** serving the same destination phone number.

- 30 If no Internet Telephony Gateways **1084**, **1081** and **1086** specifically serve

-220-

the calling area of the given destination telephone number, the directory service **1082** returns an error TCP/IP message to the Client Computer **1080**. The Client **1080** then has the option of querying the Directory Service for any Internet Telephony Gateway, not just gateways serving a particular destination telephone number.

As a refinement of this Gateway Registration scheme, Gateways can register calling rates provided for all calling areas. For example, if no gateway is available in Seattle, it may be less expensive to call Seattle from the gateway in Los Angeles, than to call Seattle from the gateway in Portland. The rates registered in the directory service can enable the directory service the lowest cost gateway to use for any particular call.

7. Vnet Call Processing

Figure **11** is a callflow diagram in accordance with a preferred embodiment. Processing commences at **1101** where the location of the directory service to receive this "on-line" message will be determined by the data distribution implementation for this customer. In some cases this may be a private database for a company or organization subscribing to a VNET service, in other cases it might be a national or worldwide database for all customers of a service provider (MCI). When the directory service receives this message from PC12 **1051**, it will update a profile entry associated with the unique ID to indicate that the user is "on-line" and is located at the specified IP address. Then, at **1102**, after successful update of the profile associated with the ID, the directory service sends a response (ACK) back to the specified IP address indicating that the message was received and processed. When the computer (PC12) receives this response message it may choose to notify the user via a visual or audible indicator.

At **1103**, a user of PC11 **1052** connects a computer to an IP network, turns on the computer and starts telephony system software. The registration

-221-

process for this computer follows the same procedures as those for PC12 **1051**. In this scenario it is assumed that the directory service receiving this message is either physically or logically the same directory service that received the message from PC12 **1051**.

5

At **1104**, when the directory service **1031** receives a message from PC11 **1052**, it initiates a similar procedure as it followed for a message for PC12 **1051**. However, in this case it will update the profile associated with the identifier it received from PC11 **1052**, and it will use the IP address it received from PC11 **1052**. Because of the updated profile information, when the acknowledgment message is sent out from the directory service, it is sent to the IP address associated with PC11 **1052**. At this point both computers (PC12 **1051** and PC11 **1052**) are "on-line" and available to receive calls.

15

At **1105**, PC12 **1051** uses its telephony system software to connect to computer PC11 **1052**. To establish this connection, the user of PC12 **1051** dials the VNET number (or other unique ID such as name, employee ID, etc).

Depending upon the implementation of the customer's network, and software package, a unique network identifier may have to be placed in this dial string. As an example, in a telephony implementation of a VNET, a subscriber may be required to enter the number 8 prior to dialing the VNET number to signal a PBX that they are using the VNET network to route the call. Once the telephony software package has identified this call as a VNET type call, it will send a translation request to the directory service. At a minimum, this translation request will contain the following information:

- The IP address of the computer (PC12 **1051**) sending this request, and
 - The VNET number (or other ID) of the computer to be dialed.

30 At **1106**, when the directory service receives this message, it uses the VNET number (or other ID) to determine if the user associated with the VNET number (or other ID) is "on-line" and to identify the IP address of the

-222-

location where the computer may be contacted. Any additional information that is available about the computer being contacted (PC11 **1052**), such as compression algorithms or special hardware or software capabilities, may also be retrieved by the directory service **1031**. The directory service **1031** then returns a message to PC12 **1051** with status information for PC11 **1052**, such as whether the computer is "on-line," its IP address if it is available and any other available information about capabilities of PC11 **1052**. When PC12 **1051** receives the response, it determines whether PC11 **1052** may be contacted. This determination will be based upon the "on-line" status of PC11 **1052**, and the additional information about capabilities of PC11 **1052**. If PC12 **1051** receives status information indicating that PC11 **1052** may not be contacted, the call flow stops here, otherwise it continues.

The following steps **1107** through **1111** are "normal" IP telephony call setup and tear-down steps. At **1107**, PC12 **1051** transmits a "ring" message to PC11 **1052**. This message is directed to the IP address received from the directory service **1031** in step **1106**. This message can contain information identifying the user of PC12 **1051**, or it may contain information specifying the parameters associated with the requested connection.

At **1108**, the message from step **1107** is received by PC11 **1052** and the receipt of this message is acknowledged by sending a message back to PC12 **1051** indicating that the user of PC11 **1052** is being notified of an incoming call. This notification may be visible or audible depending upon the software package and its configurations on PC11 **1052**.

At **1109**, if the user of PC11 **1052** accepts the call, a message is sent back to PC12 **1051** confirming "answer" for the call. If the user of PC11 **1052** does not answer the call or chooses to reject the call, a message will be sent back to PC12 **1051** indicative of the error condition. If the call was not answered, the call flow stops here, otherwise it continues.

-223-

At **1110**, the users of PC12 **1051** and PC11 **1052** can communicate using their telephony software. Communication progresses until at **1111** a user of either PC may break the connection by sending a disconnect message to the other call participant. The format and contents of this message is dependent upon the telephony software packages being used by PC12 **1051** and PC11 **1052**. In this scenario, PC11 **1052** sends a disconnect message to PC12 **1051**, and the telephony software systems on both computers discontinue transmission of voice.

Figure **12** illustrates a VNET Personal Computer (PC) to out-of-network PC Information call flow in accordance with a preferred embodiment. In this flow, the Internet telephony gateway is an out-of-network element. This means that the Internet Telephony Gateway cannot use SS7 signaling to communicate with the switch, it must simply output the VNET number to be dialed. An alternate embodiment facilitates directory services to do a translation of the VNET number directly to a Switch/Trunk and output the appropriate digits. Such processing simplifies translation in the switching network but would require a more sophisticated signaling interface between the internet gateway and the switch. This type of "in-network" internet gateway scenario will be covered in another call flow.

This scenario assumes that there is no integration between the internet and a customer premises Public Branch Exchange (PBX). If there were integration, it might be possible for the PC to go through the Internet (or intranet) to connect to an ITG on the customer's PBX, avoiding the use of the PSTN. Figure **12** is a callflow diagram in accordance with a preferred embodiment. Processing commences at **1201** where the location of the directory service to receive this "on-line" message will be determined by the data distribution implementation for this customer. In some cases this may be a private database for a company or organization subscribing to a VNET service, in other cases it might be a national or worldwide database for all

-224-

customers of a service provider (MCI).

When the directory service receives this message from PC12 **1051**, it will update a profile entry associated with the unique ID to indicate that the user is "on-line" and is located at the specified IP address. Then, at **1202**, after
5 successful update of the profile associated with the ID, the directory service sends a response (ACK) back to the specified IP address indicating that the message was received and processed. When the computer (PC12) receives this response message it may choose to notify the user via a visual or
10 audible indicator.

At **1203**, a VNET translation request is then sent to the directory services to determine the translation for the dial path to the out of network internet gateway phone. A response including the IP address and the DNIS is
15 returned at **1204**. The response completely resolves the phone addressing information for routing the call. Then, at **1205**, an IP telephony dial utilizing the DNIS information occurs. DNIS refers to Dialed Number Information Services which is definitive information about a call for use in routing the call. At **1206** an ACK is returned from the IP telephony, and at
20 **1207** an IP telephony answer occurs and a call path is established at **1208**.

1209a shows the VNET PC going offhook and sending a dial tone **1209b**, and outpulsing digits at **1210**. Then, at **1211**, the routing translation of the
25 DNIS information is used by the routing database to determine how to route the call to the destination telephone. A translation response is received at **1212** and a switch to switch outpulse occurs at **1213**. Then, at **1215**, a ring is transmitted to the destination phone, and a ringback to the PC occurs. The call is transmitted out of the network via the internet gateway
30 connection and answered at **1216**. Conversation ensues at **1217**, until one of the parties hangs up at **1218**.

-225-

Figure **13** illustrates a VNET Personal Computer (PC) to out-of-network Phone Information call flow in accordance with a preferred embodiment. In this call flow, the use of the PSTN is avoided by routing the call from the PC to the Internet/Intranet to an internet gateway directly connected to a PBX.

5

Figure **14** illustrates a VNET Personal Computer (PC) to in-network Phone Information call flow in accordance with a preferred embodiment. In this call flow, the internet telephony gateway is an in-network element. This requires that the internet gateway can behave as if it were a switch and utilize SS7 signaling to hand the call off to a switch. This allows the directory service to return the switch/trunk and outpulse digits on the first VNET lookup. This step avoids an additional lookup by the switch. In this case the directory service must have access to VNET routing information.

15

a) PC to PC

Figure **15** illustrates a personal computer to personal computer internet telephony call in accordance with a preferred embodiment. In step **1501**, a net phone user connects through the internet via an IP connection to the step **1502** MCI directory service where a look up is performed to determine how to route the call. In step **1503**, the call is terminated in the Intelligent System Platform (ISP) to determine where to send the call. IP Router is the gateway that goes into the MCI ISP to determine via the Intelligent Services Network (ISN) feature engine how to get the call through the network. In step **1504**, the call is connected through the Internet to the Net Phone user. In alternative scenario step **1504** the person at the phone is unavailable, so the calling party desired to speak with an MCI operator and the IP Router goes through the Net-Switch (interface to the voice world.) In step **1505**, the netswitch queries the call processing engine to do DSP Engine functions. In step **1506**, the call is routed through the WAN Hub to a MCI switch to an MCI Operator or voicemail in step **1507**. This preferred embodiment utilizes

30

-226-

the existing infrastructure to assist the call.

b) PC TO PHONE

Figure **16**, illustrates a phone call that is routed from a PC through the Internet to a phone. In step **1602**, the MCI Directory is queried to obtain ISN information for routing the call. Then the call is redirected in step **1603** to the ISP Gateway and routed utilizing the IP router to the call processing engine in steps **1604** and **1605**. Then, in step **1606**, the call is routed to the WAN and finally to the RBOC where Mainframe billing is recorded for the call.

c) Phone to PC

Figure **17** illustrates a phone to PC call in accordance with a preferred embodiment. In step **1701**, a phone is routed into a special net switch where in step **1702**, a call processing engine determines the DTMF tones utilizing a series of digital signal processors. Then, at step **1703**, the system looks up directory information and connects the call. If the caller is not there, or busy, then at step **1704**, the call is routed via an IP router over the switch utilizing the call processing engine in step **1705**.

d) Phone to Phone

Figure **18** illustrates a phone to phone call over the internet in accordance with a preferred embodiment. A call comes into the switch at step **1801**, and is processed by the call logic program running in the call processing engine in step **1802**. In step **1803**, a lookup is performed in the directory information database to determine routing of the call as described above. The routing includes storing a billing record in the mainframe billing application **1808**. All of the ISN features are available to the call even though the call is routed through the internet. An IP router is used at each

-227-

end of the internet to facilitate routing of the call through the internet **1804** and into the network switch. From the network switch the call is routed to a call processing engine through a WAN hub **1806** through the RBOC **1807** to the target telephone. Various DSP Engines **1803** are utilized to perform
5 digital transcoding, DTMF detection, voice recognition, call progress, VRU functions and Modem functions.

XI. TELECOMMUNICATION NETWORK MANAGEMENT

A preferred embodiment utilizes a network management system for a
10 telecommunication network for analyzing, correlating, and presenting network events. Modern telecommunications networks utilize data signaling networks, which are distinct from the call-bearing networks, to carry the signaling data that are required for call setup, processing, and clearing. These signaling networks use an industry-standard architecture and
15 protocol, collectively referred to as Common Channel Signaling System #7, or Signaling System #7 (SS7) for short. SS7 is a significant advancement over the previous signaling method, in which call signaling data were transmitted over the same circuits as the call. SS7 provides a distinct and dedicated network of circuits for transmitting call signaling data. Utilizing
20 SS7 decreases the call setup time (perceived by the caller as post-dial delay) and increases capacity on the call-bearing network. A detailed description of SS7 signaling is provided in Signaling System #7, Travis Russell, McGraw Hill (1995).

25 The standards for SS7 networks are established by ANSI for domestic (U.S.) networks, by ITU for international connections, and are referred to as ANSI SS7 and ITU C7, respectively. A typical SS7 network is illustrated in Figure **1B**. A call-bearing telecommunications network makes use of matrix switches **102a/102b** for switching customer traffic. These switches
30 **102a/102b** are conventional, such as a DMS-250 manufactured by Northern Telecom or a DEX-600 manufactured by Digital Switch

-228-

Corporation. These switches **102a/102b** are interconnected with voice-grade and data-grade call-bearing trunks. This interconnectivity, which is not illustrated in Figure **1B**, may take on a large variety of configurations.

5 Switches in telecommunications networks perform multiple functions. In addition to switching circuits for voice calls, switches must relay signaling messages to other switches as part of call control. These signaling messages are delivered through a network of computers, each of which is called a Signaling Point (SP) **102a/102b**. There are three kinds of SPs in an SS7
10 network:

- Service Switching Point (SSP)
- Signal Transfer Point (STP)
- Service Control Point (SCP)

The SSPs are the switch interface to the SS7 signaling network.

15 Signal Transfer Points (STPs) **104a...104f** (collectively referred to as **104**) are packet-switching communications devices used to switch and route SS7 signals. They are deployed in mated pairs, known as clusters, for redundancy and restoration. For example, in Fig. **1B**, STP **104a** is mated
20 with STP **104b** in Regional Cluster 1, STP **104c** is mated with STP **104d** in Regional Cluster 2, and STP **104e** is mated with STP **104f** in Regional Cluster 3. A typical SS7 network contains a plurality of STP clusters **104**; three are shown in Fig. 1 for illustrative purposes. Each STP cluster **104** serves a particular geographic region of SSPs **102**. A plurality of SSPs **102**
25 have primary SS7 links to each of two STPs **104** in a cluster. This serves as a primary homing arrangement. Only two SSPs **102** are shown homing to Regional Cluster 2 in Fig. **1B** for illustrative purposes; in reality, several SSPs **102** will home on a particular STP cluster **104**. SSPs **102** will also generally have a secondary SS7 link to one or both STPs **104** in another
30 cluster. This serves as a secondary homing arrangement.

The SS7 links that connect the various elements are identified as follows:

-229-

A links connect an SSP to each of its primary STPs (primary homing).

B links connect an STP in one cluster to an STP in another cluster.

C links connect one STP to the other STP in the same cluster.

5 D links connect STPs between different carrier networks (not illustrated).

E links connect an SSP to an STP that is not in its cluster (secondary homing).

F links connect two SSPs to each other.

10 To interface two different carriers' networks, such as a Local Exchange Carrier (LEC) network with an Interchange Carrier (IXC) network, STP clusters **104** from each carriers' network may be connected by D links or A links. SS7 provides standardized protocol for such an interface so that the signaling for a call that is being passed between an LEC and an IXC may
15 also be transmitted.

When a switch receives and routes a customer call, the signaling for that call is received (or generated) by the attached SSP **102**. While intermachine trunks that connect the switches carry the customer's call, the signaling for
20 that call is sent to an STP **104**. The STP **104** routes the signal to either the SSP **102** for the call-terminating switch, or to another STP **104** that will then route the signal to the SSP **102** for the call-terminating switch. Another element of an SS7 network are Protocol Monitoring Units (PMU) **106**, shown in Figure **2**. PMUs **106** are deployed at switch sites and provide an
25 independent monitoring tool for SS7 networks. These devices, such as those manufactured by INET Inc. of Richardson, TX., monitor the A, E, and F links of the SS7 network, as shown in Figure **2**. They generate fault and performance information for SS7 links.

30 As with any telecommunications network, an SS7 network is vulnerable to fiber cuts, other transmission outages, and device failures. Since an SS7 network carries all signaling required to deliver customer traffic, it is vital

-230-

that any problems are detected and corrected quickly. Therefore, there is an essential need for a system that can monitor SS7 networks, analyze fault and performance information, and manage corrective actions.

5 Prior art SS7 network management systems, while performing these basic functions, have several shortcomings. Many require manual configuration of network topology, which is vulnerable to human error and delay topology updates. Configuration of these systems usually requires that the system be down for a period of time. Many systems available in the industry are
10 intended for a particular vendor's PMU **106**, and actually obtain topology data from their PMUs **106**, thereby neglecting network elements not connected to a PMU **106** and other vendors' equipment.

Because prior art systems only operate with data received from proprietary
15 PMUs **106**, they do not provide correlation between PMU events and events generated from other types of SS7 network elements. They also provide inflexible and proprietary analysis rules for event correlation.

A system and method for providing enhanced SS7 network management
20 functions are provided by a distributed client/server platform that can receive and process events that are generated by various SS7 network elements. Each network event is parsed and standardized to allow for the processing of events generated by any type of element. Events can also be received by network topology databases, transmission network management
25 systems, network maintenance schedules, and system users. Referring to Figure **3**, the systems architecture of the preferred embodiment of the present invention, referred to as an SS7 Network Management System (SNMS), is illustrated. SNMS consists of four logical servers
302/304/306/308 and a plurality of client workstations **312a/312b/312c**
30 connected via a Network Management Wide Area Network (WAN) **310**. The four logical SNMS servers **302/304/306/308** may all reside on a single or a plurality of physical units. In the preferred embodiment, each logical server

-231-

resides on a distinct physical unit, for the purpose of enhancing performance. These physical units may be of any conventional type, such as IBM RS6000 units running with AIX operating system.

- 5 The client workstations **312** may be any conventional PC running with Microsoft Windows or IBM OS/2 operating systems, a dumb terminal, or a VAX VMS workstation. In actuality, client workstations may be any PC or terminal that has an Internet Protocol (IP) address, is running with X-
10 Windows software, and is connected to the WAN **310**. No SNMS-specific software runs on the client workstations **312**.

SNMS receives events from various SS7 network elements and other network management systems (NMS) **338**. It also receives network topology, configuration, and maintenance data from various external systems, as will
15 be described. The various network elements that generate events include Network Controllers **314**, International and Domestic SPs **316/102**, STPs **104**, and PMUs **106**. Network Controllers **314** are devices that switch circuits based on external commands. They utilize SS7 signaling in the same manner as an SSP **102**, but are not linked to any STPs **104**. International
20 SPs **316** support switches that serve as a gateway between a domestic and international telecommunications network. The STPs **104** may be domestic or international.

The PMUs **106** scan all the SS7 packets that pass across the SS7 circuits,
25 analyze for fault conditions, and generate network events that are then passed onto SNMS. The PMUs **106** also generate periodic statistics on the performance of the SS7 circuits that are monitored.

All SPs **102/316**, STPs **104**, PMU **106**, and SS7 Network Controllers **314**
30 transmit network events to SNMS via communications networks. This eliminates the need for SNMS to maintain a session with each of the devices. In one typical embodiment, as illustrated in Fig. **3**, an Asynchronous Data

-232-

Communications Network **320** is used to transport events from Network Controllers **314** and International SPs **316**. An IBM mainframe Front End Processor (FEP) **324**, such as IBM's 3708, is used to convert the

asynchronous protocol to SNA so it can be received by a IBM mainframe-

5 based Switched Host Interface Facilities Transport (SWIFT) system **326**.

SWIFT **326** is a communications interface and data distribution application that maintains a logical communications session with each of the network elements.

10 In this same embodiment, an X.25 Operational Systems Support (OSS) Network **328** is used to transport events from STPs **104**, SPs **102**, and PMUs **106**. These events are received by a Local Support Element (LSE) system **330**. The LSE **330**, which may be a VAX/VMS system, is essentially a Packet Assembler/Disassembler (PAD) and protocol converter used to

15 convert event data from the X.25 OSS Network **328** to the SNMS servers **302/304**. It also serves the same function as SWIFT **326** in maintaining communication sessions with each network element, thus eliminating the need for SNMS to do so. The need for both SWIFT **326** and LSE **330** illustrates one embodiment of a typical telecommunications network in

20 which different types of elements are in place requiring different transport mechanisms. SNMS supports all these types of elements.

All network events are input to the SNMS Alarming Server **302** for analysis and correlation. Some events are also input to the SNMS Reporting Server

25 **304** to be stored for historical purposes. A Control system **332**, which may be a VAX/VMS system, is used to collect topology and configuration data from each of the network elements via the X.25 OSS Network **328**. Some elements, such as STPs **104** and SPs **102**, may send this data directly over the X.25 OSS Network **328**. Elements such as the International SSP **316**,

30 which only communicates in asynchronous mode, use a Packet Assembler/Disassembler (PAD) **318** to connect to the X.25 OSS Network **328**. The Control system **332** then feeds this topology and configuration

-233-

data to the SNMS Topology Server **306**.

Network topology information is used by SNMS to perform alarm correlation and to provide graphical displays. Most topology information is received
5 from Network Topology Databases **334**, which are created and maintained by order entry systems and network engineering systems in the preferred embodiment. Topology data is input to the SNMS Topology Server **306** from both the Network Topology Databases **334** and the Control System **332**. An ability to enter manual overrides through use of a PC **336** is also provided to
10 the SNMS Topology Server **306**.

The SNMS Alarming Server **302** also receives events, in particular DS-3 transmission alarms, from other network management systems (NMS) **338**. Using topology data, SNMS will correlate these events with events received
15 from SS7 network elements. The SNMS Alarming Server **302** also receives network maintenance schedule information from a Network Maintenance Schedule system **340**. SNMS uses this information to account for planned network outages due to maintenance, thus eliminating the need to respond to maintenance-generated alarms. SNMS also uses this information to
20 proactively warn maintenance personnel of a network outage that may impact a scheduled maintenance activity.

The SNMS Alarming Server **302** has an interface with a Trouble Management System **342**. This allows SNMS users at the client
25 workstations **312** to submit trouble tickets for SNMS-generated alarms. This interface, as opposed to using an SNMS-internal trouble management system, can be configured to utilize many different types of trouble management systems. In the preferred embodiment, the SNMS Graphics Server **308** supports all client workstations **312** at a single site, and are
30 therefore a plurality of servers. The geographical distribution of SNMS Graphics Servers **308** eliminates the need to transmit volumes of data that support graphical presentation to each workstation site from a central

-234-

location. Only data from the Alarming Server **302**, Reporting Server **304**, and Topology Server **306** are transmitted to workstation sites, thereby saving network transmission bandwidth and improving SNMS performance. In alternative embodiments, the Graphics Servers **308** may be centrally
5 located.

Referring now to Figure **4**, a high-level process flowchart illustrates the logical system components of SNMS. At the heart of the process is Process Events **402**. This component serves as a traffic cop for SNMS processes.

10 Process Events **402**, which runs primarily on the SNMS Alarming Server **302**, is responsible for receiving events from other SNMS components, processing these events, storing events, and feeding processed event data to the Reporting and Display components. The Process Events process **402** is shown in greater detail in Figure **5**.

15 The Receive Network Events component **404**, which runs primarily on the Alarming Server **302**, receives network events from the various SS7 network elements (STPs **104**, SPs **102**, PMUs **106**, etc.) via systems such as SWIFT **326** and LSE **330**. This component parses the events and sends them to
20 Process Events **402** for analysis. The Receive Network Events process **404** is shown in greater detail in Figure **6**.

The Process Topology component **406**, which runs primarily on the Topology Server **306**, receives network topology and configuration data from the
25 Network Topology Databases **334**, from the SS7 network elements via the Control System **332**, and from Manual Overrides **336**. This data is used to correlate network events and to perform impact assessments on such events. It is also used to provide graphical presentation of events. Process Topology **406** parses these topology and configuration data, stores them,
30 and sends them to Process Events **402** for analysis. The Process Topology process **406** is shown in greater detail in Figure **7**.

-235-

The Define Algorithms component **408**, which runs primarily on the Alarming Server **302**, defines the specific parsing and analysis rules to be used by SNMS. These rules are then loaded into Process Events **402** for use in parsing and analysis. The algorithms are kept in a software module, and are defined by programmed code. A programmer simply programs the pre-defined algorithm into this software module, which is then used by Process Events **402**. These algorithms are procedural in nature and are based on network topology. They consist of both simple rules that are written in a proprietary language and can be changed dynamically by an SNMS user, and of more complex rules which are programmed within SNMS software code.

The Receive NMS Data component **410**, which runs primarily on the Alarming Server **302**, receives events from other network management systems (NMS) **338**. Such events include DS-3 transmission alarms. It also receives network maintenance events from a Network Maintenance Schedule system **340**. It then parses these events and sends them to Process Events **402** for analysis. The Display Alarms component **412**, which runs primarily on the Graphics Server **308** and the Alarming Server **302**, includes the Graphical User Interface (GUI) and associated software which supports topology and alarm presentation, using data supplied by Process Events **402**. It also supports user interactions, such as alarm clears, acknowledgments, and trouble ticket submissions. It inputs these interactions to Process Events **402** for storing and required data updates. The Display Alarms process **412** is shown in greater detail in Figure **8**.

The Report On Data component **414**, which runs primarily on the Reporting Server **304**, supports the topology and alarm reporting functions, using data supplied by Process Events **402**. The Report On Data process **414** is shown in greater detail in Figure **9**.

Referring now to Figure **5**, the detailed process of the Process Events

-236-

component **402** is illustrated. This is the main process of SNMS. It receives generalized events from other SNMS components, parses each event to extract relevant data, and identifies the type of event. If it is an SS7-related event, Process Events **402** applies a selected algorithm, such as create
5 alarm or correlate to existing alarm.

The first three steps **502-506** are an initialization process that is run at the start of each SNMS session. They establish a state from which the system may work. Steps **510-542** are then run as a continuous loop.

10

In step **502**, current topology data is read from a topology data store on the Topology Server **306**. This topology data store is created in the Process Topology process **406** and input to Process Events **402**, as reflected in Figure **4**. The topology data that is read has been parsed in Process Topology
15 **406**, so it is read in step **502** by Process Events **402** as a standardized event ready for processing.

20

In step **504**, the algorithms which are created in the Define Algorithms component **408** are read in. These algorithms determine what actions SNMS will take on each alarm. SNMS has a map of which algorithms to invoke for which type of alarm.

25

In step **506**, alarms records from the Fault Management (FM) reporting database, which is created in the Report on Data process **414**, are read in.
All previous alarms are discarded. Any alarm that is active against a node or circuit that does not exist in the topology (read in step **502**) is discarded. Also, any alarm that does not map to any existing algorithm (read in step **504**) is discarded. The alarms are read from the FM reporting database only within initialization. To enhance performance of the system, future alarm
30 records are retrieved from a database internal to the Process Events **402** component. Step **506** concludes the initialization process; once current topology, algorithms, and alarms are read, SNMS may begin the continuous

-237-

process of reading, analyzing, processing, and storing events.

This process begins with step **510**, in which the next event in queue is received and identified. The queue is a First In/First Out (FIFO) queue that
5 feeds the Process Events component **402** with network events, topology events, and NMS events. To reiterate, the topology data that are read in step **502** and the alarm data that are read in step **504** are initialization data read in at startup to create a system state. In step **510**, ongoing events are read
10 in continuously from process components **404**, **406**, and **410**. These events have already been parsed, and are received as standardized SNMS events. SNMS then identifies the type of event that is being received. If the event is found to be older than a certain threshold, for example one hour, the event is discarded.

15 In steps **512**, **520**, **524**, and **534** SNMS determines what to do with the event based on the event type identification made in step **510**.

In step **512**, if the event is determined to be topology data, SNMS updates the GUI displays to reflect the new topology in step **514**. Then in step **516**,
20 SNMS performs a reconciliation with active alarms to discard any alarm not mapping to the new topology. In step **518**, the new topology data is recorded in a topology data store, which is kept in the SNMS Topology Server **306**.

In step **520**, if the event is determined to be NMS data, such as DS-3 alarms
25 **338**, it is stored in the FM reporting database on the SNMS Reporting Server **304** for future reference by SNMS rules.

In step **524**, if the event is determined to be a defined SS7 network event, then in step **526** one or more algorithms will be invoked for the event. Such
30 algorithms may make use of data retrieved from Network Management Systems **338**, Network Maintenance Schedules **340**, and Network Topology **334**.

-238-

For example, when each circuit level algorithm generates an alarm, it performs a check against the Network Maintenance Schedule **340** and NMS **338** records. Each alarm record is tagged if the specified circuit is within a maintenance window (Network Maintenance Schedule **340**) or is transported on a DS-3 that has a transmission alarm (NMS **338**). While SS7 circuits run at a DS-0 level, the Network Topology Databases **334** provide a DS-3 to DS-0 conversion table. Any DS-0 circuit within the DS-3 is tagged as potentially contained within the transmission fault. Clear records from NMS **338** will cause active SNMS circuit level alarms to be evaluated so that relevant NMS **338** associations can be removed. SNMS clear events will clear the actual SNMS alarm. GUI filters allow users to mask out alarms that fit into a maintenance window or contained within a transmission fault since these alarms do not require SNMS operator actions.

15

In step **528**, active alarms are reconciled with new alarm generations and clears resulting from step **526**. In step **530**, the GUI displays are updated. In step **532**, the new alarm data is stored in the FM reporting database.

20 In step **534**, the event may be determined to be a timer. SNMS algorithms sometimes need to delay further processing of specific conditions for a defined period of time, such as for persistence and rate algorithms. A delay timer is set for this condition and processing of new SNMS events continues. When the time elapses, SNMS treats the time as an event and performs the appropriate algorithm.

25

For example, an SS7 link may shut down momentarily with the possibility of functioning again within a few seconds, or it may be down for a much greater period of time due to a serious outage that requires action. SNMS, when it receives this event, will assign a timer of perhaps one minute to the event. If the event clears within one minute, SNMS takes no action on it. However, if after the one minute timer has elapsed the event is unchanged

30

-239-

(SS7 link is still down), SNMS will proceed to take action.

In step **536**, the appropriate algorithm is invoked to take such action. In step **538**, active alarms are reconciled with those that were generated or cleared in step **536**. In step **540**, the GUI displays are updated. In step **542**, the new alarm data is stored in the FM reporting database. As stated previously, SNMS operates in a continuous manner with respect to receiving and processing events. After the data stores in steps **518**, **522**, **532**, and **542**, the process returns to step **510**.

Referring now to Figure **6**, the detailed process of the Receive Network Events component **404** is illustrated. This component collects events from the SS7 network elements via data transport mechanisms, such as the Async Data Network **320**, SWIFT **326**, X.25 OSS network **328**, and the LSE **330**. These events are received by the SNMS Alarming Server **302** in a First In/First Out (FIFO) queue. In steps **602** and **604**, events from the SS7 network elements are collected by mainframe applications external to SNMS, such as SWIFT **326** and LSE **330**, and the protocol of the event data is converted from the network element-specific protocol to SNA or TCP/IP. In one embodiment, SNMS may also have software running on the mainframe that converts the protocol to that recognizable by the SNMS Alarming Server **302**. The event data is then transmitted via SNA or TCP/IP to the SNMS Alarming Server **302**. SNMS maintains a Signaling Event List **608** of all SS7 event types that is to be processed. In step **606**, SNMS checks the Signaling Event List **608** and if the current event is found in the list, SNMS traps the event for processing. If the event is not found in the list, SNMS discards it.

In step **610**, the event is parsed according to defined parsing rules **614**. The parsing rules **614** specify which fields are to be extracted from which types of events, and are programmed into the SNMS code. The parsing of events in step **610** extracts only those event data fields needed within the alarm algorithms or displays. Also input to step **610** are scheduled events **612**

-240-

from the Network Maintenance Schedule **340**. Scheduled events **612** are used to identify each network event collected in step **602** that may be a result of scheduled network maintenance. This allows SNMS operators to account for those SS7 network outages that are caused by planned
5 maintenance.

In step **616**, the parsed event data is used to create standardized event objects in SNMS resident memory for use by other SNMS processes. Such event objects are read into the main process, Process Events **402**, in step
10 **510**.

Referring now to Figure **7**, the detailed process of the Process Topology component **406** is illustrated. This process component retrieves network topology and configuration data from three types of sources, creates
15 standardized topology data records, and stores this data for use by other SNMS processes. In particular, it feeds active topology data to Process Events **402**, running on the Alarming Server **302**, in step **502**.

In step **702**, the SNMS Topology server **306** collects topology data from three
20 different sources. It collects current connectivity and configuration data generated by the SS7 network elements via the Control system **332**. It collects topology data that has been entered into order entry and engineering systems and stored in Network Topology Databases **334**. It also accepts manual overrides **336** via workstation. The collection of data from
25 the Topology Database **334** and the Control system **332** occurs on a periodic basis, and is performed independently of the SNMS Alarming server **302**. Unlike prior art systems that use data retrieved from PMUs **106**, SNMS receives topology data from all types of network elements, including those that are not connected to a PMU **106** such as that of Figure **2**. SNMS also
30 uses data reflecting the topology of foreign networks, such as those of a Local Exchange Carrier (LEC) or an international carrier. This data is used to perform impact assessments that will allow the SNMS user to determine

-241-

facts such as which end customers may be impacted by an SS7 link outage. The type of topology data collected and used by SNMS, and for example, for the SS7 linkage of an STP **104** with a Switch/SSP **102**, data is received by network order entry and engineering systems. The data and a brief
 5 description of its contents is provided below.

	STP Link ID	Identifies each SS7 link to the STP
	Switch Link ID	Identifies each SS7 link to the Switch/SP
	STP Linkset	Identifies a trunk grouping of SS7 links to the
10	STP	
	Switch Linkset	Identifies a trunk grouping of SS7 links to the Switch/SP
	MCI/Telco Circuit ID	Identifies the SS7 link to external systems. For interfaces between two different networks, each
15	ID	(MCI ID and Telco ID) provides an identification of
		the SS7 link for each network (MCI and a Telco in this example).
20	Link Type	Identifies the type of SS7 link
	SLC	Signal Link Code

For the switched voice network supported by SS7, data is received by network order entry and engineering systems and used to perform SS7 event
 25 impact assessments:

Voice Trunk Groups	Voice trunk group supported by each SSP 102
--------------------	--

For the SS7 linkage of a domestic STP **104g** to an international STP **104h**,
 30 data is received by network order entry and engineering systems:

Circuit ID	Identifies the SS7 link to external systems
------------	---

-242-

SLC Signal Link Code

For the purpose of performing impact assessments, Local Exchange Carrier (LEC) NPA/NXX assignments and End Office to Access Tandem homing arrangements are received by a calling area database that is populated by Bellcore's Local Exchange Routing Guide (LERG).

LATA	Local Access Transport Area (conventional)
NPA/NXX	Numbering Plan Area/prefix (conventional)
10 End Office	LEC customer serving node
Access Tandem	LEC end office hub

Foreign network STP **104** clustering and SSP **102** homing arrangements are received by SS7 network elements via a control system.

15

Point Code	Identifies SS7 node (conventional)
------------	------------------------------------

Data identifying certain aspects of each network element are received by a Switch Configuration File, which resides in an external system.

20

Data mapping each network DS-0 onto a DS-3 is received by Network Topology Databases. This data is used to assign DS-3 alarms received by NMS to DS-0 level circuits.

25 Data needed to overwrite data acquired through automated processes are provided by manual overrides.

Referring now back to Figure **7** in step **704**, the various topology data are parsed to extract the data fields that are needed by SNMS algorithms. The data are then standardized into event records that can be processed by Process Events **402**.

30

-243-

In step **706**, the standardized data records are validated against other data. For example, circuit topology records are validated against node topology records to ensure that end nodes are identified and defined.

- 5 In step **708**, the topology data are stored on the Topology server **306** of Figure **3** in a relational database, such as that offered by Sybase.

- 10 In step **710**, the new topology records are passed from the Topology server **306** to the main SNMS process running on the Alarming server **302** and compared against the active configuration (i.e. configuration that is currently loaded into memory). Active alarm and GUI displays are reconciled to remove alarms that pertain to non-existent topology entries.

- 15 In step **712**, the topology is stored on the Alarming Server **302** (for use by Process Events **402**) in the form of flat files for performance reasons. At this time the flat file mirrors the Topology server **306** database from step **708**. This flat file is only accessible by the main process. In step **714**, the new topology records are loaded into active SNMS memory and new processes which require topology data now use the new configuration.

20

- Referring now to Figure **8**, the detailed process of the Display Alarms component **412** is illustrated. This process component provides the results of SNMS processing to the user (referred to as the "operator"), and accepts operator input as actions to be performed within SNMS. Therefore, the process between Display Alarms **412** and Process Events **402** is two-way. It is important to note that while there is a single Process Events process **402** running for the entire SNMS system, there is a different instance of the Display Alarms process **412** running for each operator that is logged onto SNMS. That is, each operator instigates a separate execution of Display Alarms **412**.
- 25
- 30

When an operator logs on SNMS, the first four steps, **802 - 808**, execute as

-244-

an initialization. From there, steps **810 - 838** operate as a continuous loop. The initialization provides each operator with a system state from which to work. In step **802**, the current topology is read in and displayed via Graphical User Interface (GUI). Each operator has its own GUI process that
5 is initialized and terminated based upon an operator request. Each GUI process manages its displays independently. Any status change is handled by the individual processes.

10 In step **804**, a filter that defines the specific operator view is read in. Each operator can define the view that his/her GUI process will display. Filter parameters include:

1. Traffic Alarms, Facility alarms, or both
2. Acknowledged Alarms, Unacknowledged Alarms, or both
- 15 3. Alarms on circuits within maintenance windows, Alarms on circuits that are not within a maintenance window, or both.
4. Alarms on circuits that have associated transmission alarms (DS-3 alarms via outage ids), Alarms on circuits that do not have associated transmission alarms, or both.
- 20 5. Alarms with a specified severity.
6. Alarms on nodes/circuits owned by a specified customer id.
7. Alarms on International circuits, Alarms on Domestic circuits, or both.

25 The operator's GUI displays are updated both upon initialization in step **804** and when filter changes are requested in steps **828** and **830**. Each specific operator's instance of the Display Alarms **412** process opens a connection with Process Events **402** so that only alarm records relevant to the specific operator's filter are transmitted. In step **806**, the specific operator's process
30 registers itself with Process Events **402** to identify which alarms are to be sent. In step **808**, the GUI display is presented to the operator.

-245-

- The continuous execution of Display Alarms **412** begins in step **810**. Each event that is to be retrieved and presented, as defined by the operator filter, is received and identified. In steps **812, 816, 820, 826, and 836** SNMS determines what to do with the event based on the event type identification made in step **810**. In steps **812** and **816**, if the event is determined to be an alarm update or a topology update, the operator's GUI display is updated to reflect this, in steps **814** and **818**, respectively. Then the next event is received, in step **810**.
- 10 In step **820**, if the event is determined to be an operator action, two activities are required. First, in step **822**, the operator's GUI display is updated to reflect the status change. Then, in step **824**, a status change update is sent to the main process, Process Events **402**, so that the status change may be reflected in SNMS records and other GUI processes (for other operators) can receive and react to the status changes.
- 15

In step **826**, if the event is determined to be an operator display action, then it is determined if the action is a filter change request or a display request. In step **828**, if it is determined to be a filter change request, then in step **830** the GUI process registers with Process Events **402** so that the appropriate alarms records are transmitted. In step **832**, if it is determined to be an operator display request, then in step **834** the requested display is presented to the operator. Display requests may include:

- 25
1. node detail and connection
 2. circuit connection
 3. linkset connection
 4. unknown topology alarms (alarms on objects that are not defined in the topology databases)
 - 30 5. STP pair connections
 6. Nodes contained within a LATA
 7. Home/Mate connections (for non-adjacent nodes)

-246-

8. NPA/NXX lists
9. trunk group lists
10. end office access tandem
11. rules definition help screens (aid the operator in understanding the
5 actual algorithm used in generating the alarm
12. recommended actions (operator defined actions that should be taken
when a specific alarm is received)

10 In step **836**, if the event is determined to be a termination request, then the specific operator's GUI process is terminated in step **838**. Otherwise, the next event is received in step **810**. Within the Display Alarm process, SNMS provides several unique display windows which support fault isolation, impact assessments, and trouble handling. All of the GUI displays which contain node and circuit symbols are "active" windows within SNMS (i.e.
15 screens are dynamically updated when alarm status of the node or circuit change). All the displays are possible due to the set of MCI topology sources used within SNMS. SNMS has extensive topology processing of SNMS which is used in operator displays.

20 **A. SNMS Circuits Map**

This window displays topology and alarm status information for a selected linkset. As network events are received, SNMS recognizes the relationships between endpoints and isolates the fault by reducing generated alarms. This display allows the operator to monitor a linkset as seen from both sides
25 of the signaling circuit (from the perspective of the nodes).

B. SNMS Connections Map

This window presents a cluster view of MCI's signaling network. All MCI and non-MCI nodes connected to the MCI STPs in the cluster are displayed along
30 with the associated linksets. A cluster view is important since a single STP

-247-

failure/isolation is not service impacting, but a cluster failure is since all MCI SPs have connectivity to both MCI STPs in the cluster.

C. SNMS Nonadjacent Node Map

- 5 This window presents a STP pair view of a selected LEC signaling network. All LEC SPs, STPs, and SCPs (with signaling relationships to the MCI network) connected LEC STP pair are displayed. MCI's area of responsibility does not include the LEC STP to LEC SSP signaling links, so no linksets are displayed here. This display allows the SNMS operator to
- 10 monitor a LEC signaling network as seen by the MCI nodes.

D. SNMS LATA Connections Map

- This window presents a map of all LEC owned nodes that are located within a specified LATA. As well, the MCI STP pair that serves the LATA is also
- 15 displayed along with the associated linksets (where applicable). This display allows the operator to closely monitor a specific LATA if/when problems surface within the LATA. LATA problems, while outside MCI's domain of control, can introduce problems within the MCI network since signaling messages are shared between the networks. As well, MCI voice
- 20 traffic which terminates in the specified LATA can be affected by LATA outages.

E. NPA-NXX Information List

- This window presents a list of NPX-NXX's served by a specified LEC switch.
- 25 This display is very valuable during impact assessment periods (i.e. if the specified LEC switch is isolated, which NPA-NXX's are unavailable).

F. End Office Information List

This window presents a list of LEC end office nodes which are homed to the

specific LEC access tandem. This display is very valuable during impact assessment periods (i.e. if the specified LEC tandem switch is isolated, which end offices are unavailable).

5 **G. *Trunk Group Information List***

This window presents a list of MCI voice trunks, connected to a specified MCI switch, and the LEC end office switches where they terminate. This display is very valuable during impact assessment periods (i.e. what end offices are impacted when a MCI switch is isolated). This display is also
10 available for selected LEC end office switches.

H. *Filter Definition Window*

The SNMS operator can limited the scope of his displays to:

- 15 • type of alarms that should be presented
- severity of alarms that should be presented
- acknowledged alarms, unacknowledged alarms, or both
- alarms on circuits inside a planned outage window, alarms on
 circuits outside a planned outage window or both
- 20 • alarms that are not the result of a specified transmission network
 outage
- alarms on specified customer nodes or alarms on circuits
 connected to specified customer

25 **I. *Trouble Ticket Window***

The SNMS operator can open trouble tickets on signaling alarms. These trouble tickets are opened in MCI's trouble ticketing system. Operators can also display the status of existing trouble tickets.

Referring now to Figure 9, the detailed process of the Report On Data component 414 is illustrated. This process component, which runs on the Reporting server 304, stores SNMS-processed data and provides reports.

- 5 Standardized Network Element (NE) Event Records 914 are received with location specific time stamps. In step 902, the time stamps are converted into Greenwich Mean Time (GMT) so that standardized reports can be produced.
- 10 In step 904, all data received are stored in individual database tables. Data may also be archived for long-term storage to tape or disk. This data includes SNMS-generated alarms 916, standardized topology records 918, and performance statistics from PMUs 920. It may also include non-processed data, such as DS-3 alarms from NMS 338 and network
- 15 maintenance schedule data 340.

In step 906, reports are produced. These reports may be custom or form reports. They may also be produced on demand, or per a schedule. These reports may be presented in a number of ways, including but not limited to

20 electronic mail 908, X-terminal displays 910, and printed reports 912.

XII. VIDEO TELEPHONY OVER POTS

- The next logical step from voice over the POTS is video. Today, computers are capable of making video "calls" to each other when connected to some type of computer network. However, most people only have access to a
- 25 computer network by making a call from their modem on the POTS with another modem on a computer connected to a network, so that they can then "call" another computer on the network, which is in turn connected by a modem to another network computer. It is much simpler (and efficient) to call another person directly on the POTS and have the modems
- 30 communicate with each other, without network overhead. ITU recommendation H.324 describes terminals for low bitrate (28.8kbps

-250-

modem) multimedia communication, utilizing V.34 modems operating over the POTS. H.324 terminals may carry real-time voice, data, and video, or any combination, including video telephony. H.324 terminals may be integrated into personal computers or implemented in stand-alone devices
5 such as videotelephones and televisions. Support for each media type (voice, data, video) is optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork. H.324 allows more than one channel of each type to be in use. Other Recommendations in the H.324 series include the H.223
10 multiplex (combination of voice, data and video), H.245 control, H.263 video codec (digital encoder and decoder), and G.723.1.1 audio codec.

H.324 makes use of the logical channel signaling procedures of ITU Recommendation H.245, in which the content of each logical channel is
15 described when the channel is opened. Procedures are provided for allowing each caller to utilize only the multimedia capabilities of their machine. For example a person trying to make a video (and audio) call to someone who only has audio and not video capabilities can still communicate with the audio method (G.723.1.1)
20

H.324 by definition is a point-to-point protocol. To conference with more than one other person an MCU (Multipoint Control Unit) is needed to act as a video-call bridge. H.324 computers may interwork with H.320 computers on the ISDN, as well as with computers on wireless networks.
25

A. Components of Video Telephony System

1. DSP modem pools with ACD.

A Digital Signal Processor (DSP) modem pool is a modem bank, with each modem having the ability to be programmed for extra functions (like new V.
30 modem protocols, DTMF detection, etc.) A call is routed from the MCI

-251-

switch to an ACD. The ACD keeps a matrix of which DSP modems are available. The ACD also communicates with the ISNAP which does a group select to determine which group of Agents are responsible for this call and also which of the agents are free to process this call. In an alternative embodiment, DSP resources can be deployed without an ACD, directly connected to a switch. In this embodiment, the DSP resources are managed using an NCS-based routing step.

2. Agent

10 An Agent can be a human Video Operator (video capable MTOC), or an Automated program (video ARU). The ACD knows which Agent ports are available and connects an Agent to an Agent Port.

3. Video on Hold Server

15 If the ACD has no Agent ports available, then the caller is connected to the Video On Hold Server, which has the ability to play advertisements and other non-interactive video, until the ACD finds a free Agent port.

4. Video Mail Server

20 Video-mail messages are stored here. Customers can manage their mail and record greetings to be stored on this server.

5. Video Content Engine

Video On Demand content resides on the Video Content Engine. Video stored here can be previously recorded video-conferences, training videos, etc.

-252-

6. Reservation Engine

When people want to schedule a multi-party video-conference, they can specify the participants and time of the conference on this system. Configuration can be done with the help of a human Video Operator or by some other form entry method.

7. Video Bridge

Because H.324 is a point-to-point protocol, a Multi-point Conferencing Unit (MCU) needs to manage each participants call and re-direct the video streams appropriately. MCU conferencing will be available for customers with H.324 and H.320 compliant systems.

B. Scenario

A computer or set-top TV has H.324 compliant software, and a modem for use over POTS, most likely to be 28.8kbps (V.34) or higher. One objective is to call another party. If they do not answer or are busy, the originator has the option of leaving video-mail for the destination party. Another objective is to schedule and participate in a conference with more than two participants.

C. Connection Setup

Figure **19B** illustrates a call connection setup in accordance with a preferred embodiment. There are three methods for making a video-call to someone. The first method is to simply call them (from **1** and **7** of Figure **19B**. If the destination is busy or doesn't answer, then the caller can make another call to 1 800 VID MAIL and perform the appropriate procedures as follows.

When a user dials "1 800 VID MAIL" at **1**, the ACD on the DSP modem pool will connect a switch to a modem **2** and a port to an Agent **3**. Then the user logs-in to the system with a special, custom terminal program that utilizes

-253-

the data stream part of the H.324 bandwidth (using the ITU T.120 standard), called the V-mail Data Interface (VMDI). From a graphical user interface, icon or other menu, the caller can choose to :

- browse and search a directory of video-capable MCI customers,
- 5 - call another H.324 compliant software program,
- create a video-mail for Store & Forward for later delivery,
- personalize and record their video-mail greeting messages,
- view and manage their video-mail, or
- view selections from a library of recordings (Video On Demand).

10

In an alternate embodiment, a user can dial "1 800 324 CALL" to call a number. Then, if the destination number was 1 319 375 1772, the modem dial string would be "ATDT 1 800 324 CALL ,,, 1 319 375 1772" (the comma
' , ' tells the modem to do a short pause while dialing.) When the connection
15 to 1 800 324 CALL is made, a connection is made from the originator, to an MCI switch **1**, to an ARU **5a**, selected by an ACD **2a**, **3a**.

The ARU **5a** detects DTMF tones entered through a telephone keypad or other device for generating DTMF tones to get the destination number. The
20 originator remains on hold while the ARU **5a** makes a separate call to the destination number **5a**, **6a** and **7**. If the destination answers, the originator is connected to the destination, both party's modems can connect, and the ARU **5a** is released. If the destination is busy or does not answer, the call is transferred to 1 800 VID MAIL or an Agent through the DSP modem pool **2**.
25 If there are no DTMF tones detected, the call is transferred to an Agent through the DSP modem pool **2**. The Agent will make an H.324 connection with the caller and ask for their destination number (or provide help.) The architecture for this alternative is similar to how faxes are detected and transmitted in the directlineMCI system as discussed with respect to an
30 alternative embodiment.

D. Calling the Destination

When the destination number is known, the Video On Hold Server provides the video input for the H.324 connection **4**. A new call is made from the Agent **5**, **6** to the destination number **7**. One concern that required analysis while working out a detailed embodiment required determining if modems could re-synchronize after a switch operation without going off-line. If the destination number answers and is a modem, a connection MUST be made at the same speed as the originator modem speed. After modem handshaking is performed, the ACD instructs the switch to release the agent **3**, **5** and releases the modems **2** and **6** and connects the originator to the destination **1** and **7**. The destination PC realizes that the connection is an H.324 call (not a fax or otherwise) and the video-call proceeds.

In an alternate embodiment, if the destination answers and is a modem, a connection is made. Then, two H.324 calls are using two DSP modems. The Agent can be released from both calls **3** and **5**. The incoming data from each call is copied to the other call **2** and **6**. This way, an Agent can monitor the video call for Video Store & Forward **9**. When one connection drops carrier, the video-call is complete, and the modem carrier for the remaining call is dropped.

E. Recording Video-Mail, Store & Forward Video and Greetings

If a destination number does not answer or is busy, the Video Mail Server will play the appropriate Video-Mail greeting for the owner of the destination number **8**. The caller then leaves a video-message, which is stored on the Video Mail Server. The recording of video for Store & Forward Video is exactly the same as leaving a video-message, described above. Parameters such as destination number, forwarding time, and any other audio S&F features currently available are entered through the VMDI or communicated with a human video operator (or automated video ARU.)

To record a personalized greeting for playback when someone cannot reach you because you are busy or do not answer, is similar to leaving Video-Mail.

5 The option to do this is done through the VMDI or communicated with a human video operator.

F. Retrieving Video-Mail and Video On Demand

Users have the choice of periodically polling their video-mail for new messages, or have the video-mail server call them periodically when they
10 have a new message waiting. Configuration is done through the VMDI or human video operator. Managing and checking video-mail is also performed through the VMDI or communicated with a human video operator.

Choice of video to view for Video On Demand (VOD) is through the VMDI.
15 These videos can be previously recorded video-conferences, training videos, etc. and are stored on the Video Content Engine **9**.

G. Video-conference Scheduling

A user can navigate through the VMDI or Internet **10** WWW forms, or
20 communicate with a human video operator to schedule a multi-point conference. This information is stored on the Reservation Engine **11**. The other conference participants are notified of the schedule with a video-mail, e-mail message or otherwise. There will be an option to remind all registered conference participants at a particular time (e.g. 1 hour before the
25 conference), through video-mail (or e-mail, voice-mail, paging service or any other available notification method). The MCU (video bridge) can call each participant **12**, or H.324 users can dial In to the MCU at the scheduled time
12.

XIII. VIDEO TELEPHONY OVER THE INTERNET

Figure **19E** illustrates an architecture for transmitting video telephony over the Internet in accordance with a preferred embodiment. Real-time Transmission Protocol (RTP) based video-conferencing refers to the transmission of audio, video and data encapsulated as RTP messages. For a RTP-based video-conferencing session, a end-user station first establishes a dial-up Point-to-Point (PPP) connection with the Internet which is then used to transport the RTP messages. Audio information is compressed as per G.723.1.1 audio codec (coder - decoder) standards, Video is compressed in accordance with ITU H.263 video codec standards and data is transmitted as per ITU-T.120 standards.

RTP is a protocol providing support for applications with real-time properties. While UDP/IP is its initial target networking environment, RTP is transport-independent so that it can be used over IPX or other protocols. RTP does not address the issue of resource reservation or quality of service control; instead, it relies on resource reservation protocols such as RSVP. The transmission service with which most network users are familiar is point-to-point, or unicast service. This is the standard form of service provided by networking protocols such as HDLC and TCP.

Somewhat less commonly used (on wire-based networks, at any rate) is broadcast service. Over a large network, broadcasts are unacceptable (because they use network bandwidth everywhere, regardless of whether individual sub-nets are interested in them or not), and so they are usually restricted to LAN-wide use (broadcast services are provided by low-level network protocols such as IP). Even on LANs, broadcasts are often undesirable because they require all machines to perform some processing in order to determine whether or not they are interested in the broadcast data.

-257-

A more practical transmission service for data that is intended for a potentially wide audience is multicast. Under the multicast model on a WAN, only hosts that are actively interested in a particular multicast service will have such data routed to them; this restricts bandwidth consumption to the link between the originator and the receiver of multicast data. On LANs, many interface cards provide a facility whereby they will automatically ignore multicast data in which the kernel has not registered an interest; this results in an absence of unnecessary processing overhead on uninterested hosts.

A. Components

RSVP Routers with MBONE capability for broadcast of video from the Video Content Engine and the MCI Conference Space network. MCI will have an MBONE network that multicasts locally and transmits many unicasts out the Internet.

RSVP is a network control protocol that will allow Internet applications to obtain special qualities-of-service (QOS's) for their data flows. This will generally (but not necessarily) require reserving resources along the data path(s) either ahead of time or dynamically. RSVP is a component of the future "integrated services" Internet, which provides both best-effort and real-time qualities of service. An embodiment is presented in the detailed specification that follows.

When an application in a host (end system) requests a specific QOS for its data stream, RSVP is used to deliver the request to each router along the path(s) of the data stream and to maintain router and host state to provide the requested service. Although RSVP was developed for setting up resource reservations, it is readily adaptable to transport other kinds of network control information along data flow paths.

1. Directory and Registry Engine

When people are connected to the Internet (whether through modem dial-up, direct connection or otherwise), they can register themselves in this directory. The directory is used to determine if a particular person is available for conferencing.

2. Agents

An Agent can be a human Video Operator (video capable MTOC), or an Automated program (video ARU). An Internet ACD in accordance with a preferred embodiment is designed so that Agent ports can be managed. The ACD will know which Agent ports are available and connects an Agent to an available Agent Port. If the ACD has no Agent ports available, then the caller is connected to the Video On Hold Server, which has the ability to play advertisements and other non-interactive video, until the ACD finds a free Agent port.

3. Video Mail Server

Video-mail messages are stored here. Customers can manage their mail and record greetings to be stored on this server.

4. Video Content Engine

Video On Demand content resides on the Video Content Engine. Video stored here may be previously recorded video-conferences, training videos, etc.

5. Conference Reservation Engine

When people want to schedule a multi-party video-conference, they can specify the participants and time of the conference on this system.

-259-

Configuration can be done with the help of a human Video Operator or by some other form entry method.

6. MCI Conference Space

5 This is the virtual reality area that customers can be present in. Every participant is personified as an "avatar". Each avatar has many abilities and features, such as visual identity, video, voice, etc. Avatars interact with each other by handling various objects that represent document sharing, file transferring, etc., and can speak to each other as well as see each other.

10

7. Virtual Reality Space Engine

The Conference Spaces are generated and managed by the Virtual Reality Engine. The virtual reality engine manages object manipulation and any other logical descriptions of the conference spaces.

15

B. Scenario

If a user has a current connection to the Internet. The user will utilize H.263 compliant system software utilizing RTP (as opposed to TCP) over the Internet. If the user also desires to participate in VR MCI conference-space, and create/view video-mail, the user can join a VR session.

20

C. Connection Setup

The simplest way to make a video call to another person on the Internet is to simply make the call without navigating through menus and options as an initial telephone call. However, if the destination is busy or not answering, MCI provides services for depositing messages.

25

A customer can login to a telnet server (e.g. telnet vmail.mci.com), or use a custom-made client, or the WWW (e.g. http://vmail.mci.com). The services menu is referred to as the V-Mail Data Interface (VMDI), similar to the VMDI

-260-

available when dialing through POTS as described above.

From a menu, the caller can choose to:

- browse and search a directory of video-capable MCI customers,
- 5 - call another H.263 compliant software program,
- create a video-mail for Store & Forward for later delivery,
- personalize and record their video-mail greeting messages,
- view and manage their video-mail, and
- view selections from a library of recordings (Video On Demand).

10

When a user has specified a party to call by indicating the destination's name, IP address or other identification, the Directory is checked. It is possible to determine if a destination will accept a call without actually calling; so, since it can be determined that the destination will accept a call,

15 the originator's video client can be told to connect to the destination. If the callers are using a WWW browser (e.g. Netscape Navigator, Microsoft Internet Explorer, internetMCI Navigator, etc.) to access the VMDI, then a call can be automatically initiated using Java, JavaScript or Helper App. If a call cannot be completed, there will be a choice to leave video-mail.

20

D. Recording Video-Mail, Store & Forward Video and Greetings

If an Agent determines that a destination party is not available (off-line, busy, no answer, etc.), the Video Mail Server plays an appropriate Video-Mail greeting for the owner of the destination number **8**. The caller then

25 leaves a video-message, which is stored on the Video Mail Server. The recording of video for Store & Forward (S&F) Video is exactly the same as leaving a video-message, described above. Parameters such as destination number, forwarding time, and any other audio S&F features currently available are entered through the VMDI or communicated with a human

30 video operator (or automated video ARU.)

-261-

Customers may record their own personalized greetings to greet callers that cannot reach them because they are busy or do not answer. This is accomplished in a manner similar to leaving Video-Mail, through the VMDI or communicated with a human video operator.

5

E. Retrieving Video-Mail and Video On Demand

Users have the choice of periodically polling their video-mail for new messages, or having the video-mail server call them periodically when they have a new message waiting. Configuration is done through the VMDI or human video operator. Managing and checking video-mail is also performed through the VMDI or communicated with a human video operator. A choice of video to view for Video On Demand (VOD) is provided through the VMDI. These videos can be previously recorded video-conferences, training videos, etc. and are stored on the Video Content Engine.

15

F. Video-conference Scheduling

A user can navigate through the VMDI or Internet WWW forms, or communicate with a human video operator to schedule a conference in the Conference Space. The information is stored on the Conference Reservation Engine 8. The other conference participants are notified of the schedule with a video-mail, e-mail message or otherwise. An optional reminder is provided for all registered conference participants at a particular time (e.g. 1 hour before the conference), through video-mail (or e-mail, voice-mail, paging service or any other available notification method).

25

G. Virtual Reality

For multiple party conferences, a virtual meeting place can be generated by the Virtual Reality Space Engine. The implementation of the interface includes an embodiment based on VRML. Each person is in control of an

-262-

“avatar.” Each avatar can have many different features such as visual representation (static representation or live video “head”) and audio (voice or music). Data exchange and collaboration are all actions that can be performed in each VR conference room. The private MBONE network allows the multi-casting of conference member’s data streams. Since everyone has a different view when interacting in VR-space, the VR Space Engine can optimize the broadcast of everyone’s incoming H.263 streams to everyone else by multi-casting only those avatar streams in view for each particular avatar.

10 **XIV. VIDEO-CONFERENCING ARCHITECTURE**

MCI Video-Conferencing describes an architecture for multimedia communications including real-time voice, video and data , or any combination, including video telephony. The architecture also defines inter-operation with other video-conferencing standards. The architecture also defines multipoint configurations and control, directory services and video mail services.

A. Features

Video-Conferencing architecture is a multimedia services system and is designed to provide a number of features and functions including,

- 20 • Point-to-Point Video Telephony
- Multimedia video-conferencing with a MCU for control and multimedia information processing
- Support for Gateways for interworking with other video-conferencing systems based on ITU H.320 and ITU H.324
- 25 standards
- Support for real-time voice, video and data or any combination
- Multimedia information streams are transported between the end-user terminals using standard transport protocol RTP
- Support for dynamic capability exchange and mode preferences,
- 30 like ITU H.263 video and ITU G.723 audio, between end-user

-263-

terminals

Figure **19C** illustrates a Video-Conferencing Architecture in accordance with a preferred embodiment. The components and details of the video-conferencing architecture are detailed below.

B. Components

The Video-Conferencing System is comprised of a set of components including,

- End-User Terminals
- LAN Interconnect System
- ITU H.323 Server
- Support Service Units

1. End-User Terminals

The end-user terminals are the end points of communication. Users communicate and participate in video conferences using the end-user terminals. End-user terminals, including ITU H.323 terminals **1** & **8**, ITU H.320 terminal **9** and ITU H.324 terminal **10**, are interconnected through the ITU H.323 Server which provides the call control, multi-point control and gateway functions. End-User terminals are capable of multimedia input and output and are equipped with telephone instruments, microphones, video cameras, video display monitors and keyboards.

2. LAN Interconnect System

The LAN Interconnect System **3** is the interface system between the MCI Switch Network **2** and the different H.323 Systems including H.323 Server **4**, Video Content Engine **5**, Video Mail Server **6** and also the H.323 Directory Server **7**.

-264-

End-User terminals participating in video-telephony sessions or video-conferencing sessions establish communication links with the MCI switch network and communicate with the H.323 Server through the LAN Interconnect System. The LAN Interconnect system provides ACD-like
5 functionality for the H.323 video-conferencing system.

3. ITU H.323 Server

The H.323 Server 4 provides a variety of services including call control, multipoint control, multipoint processing, and gateway services for
10 interworking between terminals supporting different video-conferencing standards like ITU H.320 and ITU H.324.

The H.323 Server is comprised of a set of individual components which communicate with each other and with the other external systems like end-
15 user terminals, video mail server and H.323 directory server. The different components of the H.323 Server include:

- H.323 Gatekeeper
- Operator Services Module
- H.323 Multipoint Control Unit (MCU)
- 20 • H.323 Gateway

4. Gatekeeper

The H.323 Gatekeeper provides call control services to the H.323 terminals and Gateway units. The Gatekeeper provides a variety of services including:

- 25 • Call Control Signaling with terminals, gateways and MCU;
- Admissions Control for access to the video-conferencing system;
- Call Authorization ;
- Bandwidth control and management;
- Transport Address Translation for translating addresses between
30 different kinds of interworking video-conferencing systems;

- Call Management of on-going calls;
- Interfaces with the Directory Server[7] to provide directory services; and
- Interfaces with the Video Mail Server[6] for video mail services.

5

The Gatekeeper uses the ITU H.225 stream packetization and synchronization procedures for the different services, and is tightly integrated with the Operator Services Module for offering manual operator services.

10

5. Operator Services Module

The Operator Services Module offers manual/automatic operator services and is tightly integrated with the gatekeeper. The manual or the automatic operator terminal, located elsewhere on the LAN, interacts with the gatekeeper through the Operator Services Module to provide all the required operator services.

15

6. Multipoint Control Unit (MCU)

The MCU is comprised of the Multipoint Controller and the Multipoint Processor and together provides multipoint control and processing services for video-conferences. The multipoint controller provides control functions to support conferences between three or more terminals. The multipoint controller carries out capabilities exchange with each terminal in a multipoint conference. The multipoint processor provides for the processing of audio, video and/or data streams including mixing, switching and other required processing under the control of the multipoint controller. The MCU uses ITU H.245 messages and methods to implement the features and functions of the multipoint controller and the multipoint processor.

20

25

7. Gateway

The H.323 Gateway provides appropriate translation between the various transmission formats. The translation services include,

- Call Signaling message translation between H.225 and H.221 which is the part of the H.320 system;
- Communication procedures translation between H.245 and H.242; and
- Translation between the video, audio and data formats like H.263, H.261, G.723, G.728 and T.120.

The H.323 Gateway provides conversion functions for transmission format, call setup and control signals and procedures.

8. Support Service Units

The Support Service Units include the H.323 Directory Server **7**, the Video-Mail Server **6** and the Video Content Engine **5** which interact with the H.323 Server for providing different services to the end-user terminals. The H.323 Directory Server provides directory services and interacts with the gatekeeper unit of the H.323 Server. The Video Mail Server is the repository of all the video mail generated by the H.323 system and interacts with the gatekeeper unit of the H.323 server for the creation and playback of video mail. The Video Content Engine is the repository of all other types of video content which can be served to the end-user terminals. The Video Content Engine interacts with the gatekeeper unit of the H.323 Server.

C. Overview

The H.323 based video-conferencing architecture completely describes an architecture for multimedia communications including real-time voice, video and data, or any combination including video telephony. Users with H.323 terminals can participate in a multimedia video-conferencing session, a point-to-point video telephony session, or an audio only session with other

-267-

terminal users not equipped with video facilities. The architecture also includes gateways for interworking with other video-conferencing terminals based on standards like ITU H.320 and ITU H.324.

- 5 The architecture includes a directory server for offering complete directory services including search facilities. A video mail server is an integral part of the architecture providing for the recording and playback of video mail. A video content engine is also part of the overall architecture for offering multimedia content delivery services.

10

- H.323 terminals participating in a video-conferencing or a video telephony session communicate with the H.323 server through the MCI switch network. The H.323 server offers a variety of services including call control, information stream delivery, multi-point control and also gateway services
15 for interworking with H.320 or H.324 terminals. The server also offers directory services and video mail services.

- A H.323 terminal initiating a video call establishes a communication link with the H.323 Server through the MCI switch network. On admission to
20 the network by the H.323 server, the server offers a directory of other available terminals to the call initiating terminal which selects a destination terminal or a destination group to participate in a video conference. The server then sets up a communication link with the selected destination terminal or terminals and finally bridges the calling terminal and the called
25 terminal/terminals. If the destination terminal is unavailable or busy, the server offers the calling terminal an option to deposit a video mail. The server also notifies the recipient of the video mail and offers the recipient services for retrieval of the video mail on-demand. Additional services like content delivery on-demand to H.323 terminals are also offered and
30 controlled by the H.323 server.

D. Call Flow Example

The Call Flow for the H.323 architecture based video-conferencing is explained in detail for different call types including, Point-to-Point Calls including calls to other H.323, H.320 and H.324 terminals; and Multipoint
5 Video-Conference Calls.

Figure **19C** illustrates various call flows in accordance with a preferred embodiment.

1. Point-to-Point Calls

10 a) Case 1: H.323 Terminal to another H.323 Terminal

A call initiating H.323 terminal **1** initiates a call to another H.323 terminal[**8**] through the MCI Switch Network. The gatekeeper is involved in controlling the session including call establishment and call control. The Terminal end-user interface is any commercially available Web-browser.

15

- Calling terminal **1** initiates a dial-up call to the MCI Switch network;
- the call is terminated on the H.323 Gatekeeper module of the H.323 Server **4** through the LAN Interconnect **3** system;
- 20 • a PPP link is established between the calling terminal and the Gatekeeper **4** on a well-know unreliable transport address/port;
- Calling terminal sends a admission request message to the Gatekeeper[**4**]
- The Gatekeeper **4** sends an admission confirm message and
25 communicates with the Directory Server **7** and sends back directory information to calling terminal for display at the calling terminal, and the directory information is displayed as a web-page along with a choice of calling modes including Point-to-Point or Conference mode;
- 30 • the admissions exchange is followed by the setting up of a reliable

-269-

- connection for H.225 call control messaging on a well known port;
- the terminal user chooses the point-to-point mode and also chooses the destination of the call. This is the setup request message;
 - 5 • the gatekeeper **4** together with the operator services module/operator proceeds with calling the called terminal **8** with a setup request;
 - if setup request fails, the gatekeeper **4** informs the calling terminal **1** of the failure and provides an option for the calling terminal **1** to
10 leave a video mail;
 - if the user at calling terminal **1** chooses to leave a video mail for user at the destination terminal **8**, the gatekeeper **4** establishes a connection with the Video Mail Server **6** and receives a reliable port address from the mail server **6** for a H.245 connection;
 - 15 • the gatekeeper **4** additionally establishes a connection for H.225 call control with the video mail server **6**.
 - the gatekeeper **4** in-turn sends a reliable port address to calling terminal **1** for H.245 control channel. The gatekeeper **4** may be involved in H.245 control channel communications;
 - 20 • the calling terminal **1** establishes a reliable connection for H.245 control channel and H.245 procedures like capability exchange, mode preferences, etc. are carried out;
 - after the capabilities exchange, H.245 procedures will be used to establish logical channels for the different media streams;
 - 25 • the capabilities exchange also involves determination of dynamic port addresses for the transport of the different media streams;
 - the media streams are transported over the dynamic ports in the various logical channels;
 - once the terminal has completed the video mail, it closes the logical
30 channel for video after stopping transmission of the video stream;
 - data transmission is stopped and logical channel for data is closed;

-270-

- audio transmission is stopped and logical channel for audio is closed;
- H.245 call clearing message is sent to the peer entity;
- calling terminal **1** transmits a disconnect message on the H.225 port to the gatekeeper **7** which in turn sends the disconnect message to the video mail server **6**;
- the disconnect messages are acknowledged and the call is disconnected;
- if the setup request is a success, called terminal **8** responds with a connect message which include a reliable port address for H.245 connection;
- the gatekeeper **4** responds to the calling terminal **1** with the connect message along with the port address for the H.245 control channel communications;
- calling terminal **1** sets up a connection for H.225 call control signaling with the gateway **4**, establishes another connection for H.245 control channel communications and responds to the gateway **4** with connect acknowledgment message;
- the gatekeeper **4** in-turn sends the connect acknowledgment message to called terminal **8**.
- called terminal **8** now sets up a H.225 call control connection and also establishes another connection for H.245 with the gatekeeper **4** for control channel communications;
- the terminals, having established a H.245 control channel for reliable communication, exchange capabilities and other initial procedures of H.245, and an audio channel may be optionally opened before the capabilities exchange;
- following the capabilities exchange, logical channels over dynamic ports are established for each of the media streams;
- once the media logical channels are open over dynamic ports, media information can be exchanged;

-271-

- during the session, H.245 control procedures may be invoked for changing the channel structure like mode control, capability, etc.;
- also H.225 control channel is for specific procedures as requested by the gatekeeper[4] including call status, bandwidth allocation, etc.;
- for termination, either terminal may initiate a stop video message, discontinue video transmission and then close the logical channel for video;
- data transmission is discontinued and the logical channel for data is closed;
- audio transmission is discontinued and logical channel for audio is closed;
- H.245 end session message is sent and transmission on the control channel is stopped and the control channel is closed;
- terminal receiving the end session message will repeat the closing procedures and then H.225 call signaling channel is used for call clearing; and
- terminal initiating the termination will send a disconnect message on the H.225 control channel to the gatekeeper 4 which in turn sends a disconnect message to the peer terminal. The peer terminal acknowledges the disconnect which is forwarded to the initiating terminal and the call is finally released.

b) Case 2: H.323 Terminal to H.320 Terminal

A call initiated from a H.323 terminal 1 invokes a call to a H.320 terminal 9 through an MCI Switch Network. The gatekeeper along with the gateway is involved in controlling the session including call establishment and call control. A terminal end-user interface is any of the commercially available Web-browsers or a similar interface.

The call flow is similar to a H.323 terminal calling another H.323 terminal as

-272-

explained in the previous case except that a gateway **4** component is introduced between the gatekeeper **4** and the called terminal **9**. The gateway transcodes H.323 messages including audio, video, data and control to H.320 messages and vice-versa. If the H.320 terminal **9** initiates a call to a H.323 terminal[**1**], the initial dial-up routine is performed by the gateway and then the gatekeeper takes over the call control and the call proceeds as explained in the previous case.

c) Case 3: H.323 Terminal to H.324 Terminal

- 10 Call initiating H.323 terminal **1** initiates a call to a H.324 terminal **10** through the MCI Switch Network. The gatekeeper along with the gateway is involved in controlling the session including call establishment and call control. The Terminal end-user interface is a Web-browser or a similar interface.
- 15 The call flow is similar to a H.323 terminal calling another H.323 terminal as explained in the previous case except that a gateway **4** component is introduced between the gatekeeper **4** and the called terminal **9**. The gateway **4** transcodes H.323 messages including audio, video, data and control to H.324 messages and vice-versa.
- 20 If the H.324 terminal **10** initiates a call to a H.323 terminal **1**, the initial dial-up routine is performed by the gateway and then the gatekeeper takes over the call control and the call proceeds as explained in the previous case.

25 2. Multipoint Video-Conference Calls

- In the case of multipoint video-conference, all the terminals exchange initial call signaling and setup messages with the gatekeeper **4** and then are connected to the Multipoint Controller **4** for the actual conference including H.245 control channel messaging through the gatekeeper **4**.
- 30 The following are the considerations for setting up a conference:

-273-

- After the initial admission control message exchange, the users are presented with a web page with information about conference type and a dynamic list of participants.
- 5 • Participants joining later are presented with a web page with conference information and also are requested to enter authentication information
- All users get connected to the multipoint controller[4] through the gatekeeper[4]
- 10 • The multipoint controller[4] distributes information among the various participants

E. Conclusion

The video-conferencing architecture is a total solution for multimedia communications including real-time voice, video and data, or any
15 combination, including point-to-point video telephony. The architecture defines interworking with other systems utilizing ITU recommendations.

Additional services including directory services and video mail services are also part of the overall architecture.

20

XV. VIDEO STORE AND FORWARD ARCHITECTURE

The Video Store and Forward Architecture describes a video-on-demand content delivery system. The content may include video and audio or audio
25 only. Input source for the content is from the existing video-conferencing facility of MCI or from any video/audio source. Input video is stored in a Digital Library in different standard formats like ITU H.320, ITU H.324, ITU H.263 or MPEG and delivered to the clients in the requested format. Delivery is at different speeds to the clients either on the Internet or on dial-up lines
30 including ISDN and with a single storage for each of the different formats.

A. Features

The Video Store and Forward Architecture is designed with a rich set of features and functionality including:

- 5 • Delivers Video and Audio on demand;
- Supports different compression and transmission standards including ITU H.320, ITU H.324, MPEG and ITU H.263 on both IP (Internet Protocol) and RTP (Real Time Transport Protocol);
- 10 • Supports content delivery on the Internet, by dial-up ISDN lines and by low speed (28.8kbps) Analog Telephone lines;
- Supports single source of content and multiple storage and delivery formats and multiple delivery speeds; and
- Supports Content Management and Archival in multiple formats.

B. Architecture

Figure **19D** is a Video Store and Forward Architecture in accordance with a preferred embodiment.

C. Components

20 The Video Store and Forward architecture can be completely described by the following components.

- Content Creation and Transcoding.
- Content Management and Delivery.
- Content Retrieval and Display.

1. Content Creation and Transcoding

25 Input sources include analog video, video from Multi-Point Control Unit (MCU) and other video sources **1a** and **1b**. Input content is converted to standard formats like ITU H.261, ITU H.263, ITU H.320, ITU H.263, ITU H.324, MPEG and also formats to support delivery of H.263 over RTP and

-275-

H.263 over an Internet Protocol **2** and **3**. Input can initially be coded as H.263 and optionally transcoded into the various other formats and stored **2**. The transcoded content is stored on different servers, one for each content type to serve the various clients each supporting a different format

5 **5a, 5b, 5c, 5d, 5e and 5f.**

2. Content Management and Delivery

Content is stored on different servers with each server supporting a specific format and is managed by a Digital Library consisting of:

- 10 - Index Server for managing the indexes and archival of content **4**,
- Object Servers for storage of content **5a, 5b, 5c, 5d, 5e and 5f**,
- Proxy Client as a front end to the Index and Object Server and interacting with the different clients requesting for content **6**.

15 Content Delivery is by:

- Internet,
- Dial-up ISDN lines,
- Dial-up Analog Telephone lines at 28.8kbps, and

20 Content format is either a MPEG Stream, H.320 Stream, H.324 Stream, or a H.263 Stream transported over IP or RTP.

3. Content Retrieval and Display

Content Retrieval is by clients supporting various formats:

- 25 - MPEG Client - **7a**;
- ITU H.263 Client supporting RTP - **7b**;
- ITU H.263 Client supporting IP - **7c**;
- ITU H.320 Client - **7d**; and
- ITU H.324 Client - **7e**.

30

-276-

Content is retrieved by the different clients on demand and displayed on a local display.

Clients support VCR like functions like fast-forward, re-wind, etc.

5

D. Overview

Analog Video from different sources and H.320 video from an MCU is received as input and transcoded into various formats as required like ITU H.324, ITU H.261, ITU H.263 or MPEG and stored on the different Object

10 Servers dedicated for each of the formats. The Object Servers are in turn managed by the Index Server and are together called a Digital Library. Any request from the clients for content is received by the Index Server and in turn serviced by the Object Server through a Proxy Client.

15 The Index Server or the Library Server respond to requests from the proxy client and store, update and retrieve objects like H.261, H.263 or MPEG multimedia information on the object servers. Then they direct the object server to deliver the retrieved information back to the proxy client. The Index Server has the complete index information of all the different objects

20 stored on the object servers and also information on which of the object server the information is residing on. The index information available on the Index Server is accessible by the proxy client for retrieval of multimedia content from the different object servers. Security and access control is also

25

The Object Servers are an integral part of the Digital Library providing physical storage and acting as the repository for the multimedia content, including the video-conferencing information stream from the conferencing facilities. The multimedia content is stored in standard formats which can

30 be retrieved by the proxy client on demand. Each of the Object Servers are dedicated for a specific format of multimedia content like H.261, H.263,

-277-

MPEG, etc. The organization and index information of the multimedia content including information about the specific object server dedicated for a multimedia format is managed by the index server. The Object Server delivers the stored multimedia content to the proxy client upon receiving
5 specific instructions from the index server.

The Proxy Client is the front end of the digital library and is accessed by all the clients through the Internet for on-demand multimedia content. The Proxy Client also is a World Wide Web (WWW) Server and delivers a page to
10 the clients when accessed. The clients interact with the Proxy Client and thereby with the Digital Library through the WWW pages. Clients request multimedia content by interacting with the WWW pages. The Proxy Client receives the request from the clients through the WWW pages and processes the request. The Proxy Client then communicates with the index server with
15 object queries as requested by the client. The index server then communicates with one of the object servers dedicated to the requested multimedia format and, based on the index information available at the index server, directs the object servers to deliver the requested multimedia content to the Proxy Client. The Proxy Client receives the multimedia
20 content from the object server and delivers it to the client making the request.

The Clients connect to the Servers either through the Internet or by dial-up connections on an ISDN line or an Analog line at 28.8 Kbps depending on
25 the video format requested and the client capabilities. A H.320 client connects by an ISDN line and a H.324 client requests services on an analog telephone line at 28.8 Kbps. A MPEG client or a H.263 client using RTP or a H.263 client using IP request services through the Internet. The front-ends for multimedia content query and display like the WWW browsers are
30 integrated as a part of the Client and provide an easy-to-use interface for the end-users.

-278-

A request for video from the client is received by the proxy client which routes the request to the Index Server which in turn processes the request and communicates with a specific Object Server in addition to indexing the content for delivery. The Object Server delivers the requested content to the client through the Internet. In the case of the dial-up links, the content is delivered back on the already established link.

In sum, the Video Store and Forward architecture describes a comprehensive system for the creation, transcoding, storage, archiving, management and delivery of video and audio or audio on demand. The delivery of video and audio or audio will be on the Internet or by ISDN or Analog Telephone dial-up lines. Content including video and audio or audio is delivered at various data rates from individual storage locations, each serving a different delivery speed.

XVI. VIDEO OPERATOR

A. Hardware Architecture

Figure 96 shows the system hardware for allowing a video operator to participate in a video conference or video call, providing numerous services to the video callers. Among the services provided are: answering incoming video calls or dialing out to customer sites; accessing a system for maintaining video conference schedules, joining callers using Bandwidth on Demand Interoperability Group ("BONDING") calls or International Telecommunication Union-Telecommunication Standardization Sector ("ITU-T") standard H.320 Multi-rate Bearer Service (MRBS) Integrated Services Digital Network ("ISDN") calls into a video conference or video call; monitoring, viewing and recording any video conference or video call; playing back video conferences or video calls recorded earlier; and offering assistance to or responding to inquiries from video conference callers during video conferences or video calls.

-279-

The system hardware is comprised of a Video Operator Terminal **40001**, a Call Server **40002**, a multimedia hub ("MM Hub") **40003**, wide area network hubs ("WAN Hubs") **40004**, a multi-point conferencing unit ("MCU") **40005**,
5 a BONDING Server **40006**, a Client Terminal **40007**, and a switching network ("MCI") **40008**.

In one embodiment, the Video Operator Terminal **40001** is a Pentium-based personal computer with a processing speed of 90 MHz or greater, 32MB
10 RAM, and a hard disk drive with at least 1.0GB storage space. The operating system in this embodiment is Microsoft's Windows 95. Special features include Incite Multimedia Communications Program ("MCP") software, an H.320 video coder/decoder ("codec") card for audio and video compression (e.g. Zydacron's Z240 codec), and an isochronous Ethernet
15 ("isoEthernet") network interface card. Incite's MCP manages the isoEthernet network interface card to create the equivalent of 96 ISDN B-channels in isochronous channels for transmission of video signals.

The Call Server **40002** in this embodiment is a Pentium-based personal
20 computer with a processing speed of 90 MHz or greater, 32MB RAM, and a hard disk drive with at least 1.0GB storage space. The operating system is Microsoft's Windows NT Server. Special features include the Incite Call Server services and an Ethernet network interface card.

25 Different embodiments of the system accommodate any model of MM Hub **40003** and any model of WAN Hub **40004**. In one embodiment, the MM Hub **40003** is the Incite Multimedia Hub, and the WAN Hub is the Incite WAN Hub. The MM Hub **40003** is a local area network ("LAN") hub that connects, via numerous ports supporting isoEthernet interfaces each with a
30 bandwidth consisting of 96 full-duplex B-channels, to personal computers such as the Video Operator Terminal **40001** and the BONDING Server **40006**, to WAN Hubs **40004**, or to other cascaded MM Hubs. In addition,

-280-

the MM Hub **40003** can accept up to ten Mbps of Ethernet data via an Ethernet interface such as the one from the Call Server **40002**. The WAN Hub **40004** acts as an interface between an MM Hub **40003** and a public or private switched network such as MCI **40008**, enabling video conferencing to extend beyond the WAN or LAN containing the MM Hub **40003** and WAN Hub **40004**.

Different embodiments of the system also accommodate various manufacturers' MCU **40005** devices. The function of an MCU **40005** is to allow video conference callers using a variety of different devices, possibly communicating over different circuit-based digital networks, to communicate with one another in a single video conference. For example, one embodiment employs VideoServer's Multimedia Conference Server ("MCS"), which mixes audio to allow any one video conference caller to hear the complete video conference discussion and processes video to allow each video conference caller to see all other callers simultaneously.

In one embodiment, the BONDING Server **40006** is a Pentium-based personal computer with a processing speed of 90 MHz or greater, 32MB RAM, and a hard disk drive with at least 1.0GB storage space. The operating system in this embodiment is Microsoft's Windows 95. Special features include Incite BONDING Server software, a Digital Signal Processor ("DSP") card (such as Texas Instrument's "TMS320C80" DSP), and an isoEthernet network interface card. Where a Client Terminal **40007** makes BONDING or Aggregated video calls, the BONDING Server **40006** converts the calls to multi-rate ISDN calls used within the video operator platform.

In a preferred embodiment, the Client Terminal a Pentium-based personal computer with a processing speed of 90 MHz or greater, 32MB RAM, and a hard disk drive with at least 1.0GB storage space. The operating system is Microsoft's Windows 95 in this embodiment, and the Client Terminal **40007** is equipped with audio and video equipment making it compatible with ITU-

-281-

T standard H.320.

In this embodiment, the switching network is an integrated services digital network ("ISDN") provided by MCI **40008**.

5

The Video Operator Terminal **40001** is connected to the MM Hub **40003** via an isoEthernet interface with a bandwidth of 96 full-duplex B-channels, which allows each video operator to manage up to eight video conferencing clients, each client employing a Client Terminal **40007**. The MM Hub

10

40003 is connected to WAN Hubs **40004** via similar isoEthernet local area network ("LAN") connections. One WAN Hub **40004** connects through MCI **40008** to an MCU **40005** via multi-rate ISDN interfaces. Another WAN Hub **40004** connects to MCI **40008** via a multi-rate ISDN interface, and MCI

15

connects to each Client Terminal **40007** via a BONDING or multi-rate ISDN interface. In a three-way connection, the MCU **40005**, the Call Server **40002** and the MM Hub **40003** are connected to one another through an Ethernet wide area network ("WAN") **40009**. The MM Hub **40003** is also connected to a BONDING Server **40006** via an isoEthernet interface with a bandwidth of 248 B-channels in full "iso" mode.

20

B. Video Operator Console

Figure **97** shows one embodiment of the system for enabling a video operator to manage video conference calls, which includes a Video Operator Console system **40101** and external systems and interfaces **40108** through

25

40117.

The Video Operator Console system **40101** is comprised of a Graphical User Interface ("GUI") **40102**, a Software System **40103** and a Media Control system **40107**. The GUI **40102** interacts with both the Software System

30

40103 and the Media Control system **40107** to allow a video operator to perform all functions of the video operator invention from the Video

-282-

Operator Terminal [**40001** Figure **96**] using the Video Operator Console system **40101**.

The Software System **40103** implements the following systems: a

- 5 Scheduling system **40104** which manages the video operator's schedule; a Recording and Playback system **40105** which records the audio and video input from any call and plays back audio and video input through any call; and a Call System Interface **40106** which acts as an application program interface with the Incite MCP application to manage individual calls by
- 10 performing switching functions such as dial and hold.

- The Scheduling system **40104** is connected via an Open Database Connectivity ("ODBC") interface **40108** to a Video Operator Shared Database **40111**, which is in turn connected via an interface between VOSD
- 15 and VRS **40114** to a Videoconference Reservation System ("VRS") **40115**. The VRS **40115** submits video conference schedules, conference definitions and site definitions to the Video Operator Shared Database **40111** via the interface **40114** either on a regular basis or on demand by a database agent system within the Video Operator Shared Database **40111**. The Video
 - 20 Operator Shared Database **40111**, residing in a different computer from that containing the Video Operator Console **40101** in a preferred embodiment, stores all conference and site information such that each Video Operator Console **40101** can retrieve the necessary conference and site configurations for any video conference call. In an alternative embodiment
 - 25 of the external systems associated with the internal Scheduling system **40104**, the Video Operator Shared Database **40111** and VRS **40115** may be merged into a single system.

- The Recording and Playback system **40105** communicates via a Dynamic
- 30 Data Exchange ("DDE"), Object Linking and Embedding ("OLE") or Dynamic Link Library ("DLL") interface **40109** with a Video Operator Storage and Playback system **40112** located locally in the Video Operator Terminal

-283-

[**40007** Figure **96**]. The Video Operator Storage and Playback system is comprised of a uni-directional recording device **40116** conforming to ITU-T standard H.320 and a uni-directional playback device **40117** conforming to ITU-T standard H.320. Conference calls are recorded by transmitting the digitized audio and video signals from the Video Operator Console **40101** to the H.320 recorder **40116**. Conference calls are played back by retrieving a previously recorded conference call from disk storage and transmitting the audio and video signals from the H.320 playback device **40117** to the Video Operator Console.

The Call System Interface system **40106** communicates via a DDE interface **40110** with the Incite MCP application **40113** to manage switching functions such as dial, hold, etc.

The Media Control system **40107** allows the GUI **40102** to communicate directly with external components to manage the GUI **40102** presentation of audio and video. In the embodiment shown in Figure **401**, the Media Control system **40107** communicates via a DDE interface **40110** with the Incite MCP application **40113**. The Incite MCP application **40113** provides all necessary call setup features and multimedia features such as video window placement and audio control through the DDE interface **40110** to the internal Media Control system **40107**, and on to the GUI **40102**.

Figure **98** shows a second embodiment of the system for enabling a video operator to manage video conference calls, which includes a Video Operator Console system **40101** and external systems and interfaces **40108** through **40117** and **40203** through **40216**. In this embodiment, however, the Software System **40103** is compatible with not only VideoServer's "MCS" **40215** MCU, but also other manufacturers' MCU applications. Thus the internal software system MCU control **40201**, the external software system MCU Control System **40208**, the MCUs themselves **40214** and **40215**, and the interfaces between them **40206**, **40210** and **40211**, appear in Figure

-284-

98. In addition, because not only the Incite MCP **40113** application but also "Other programs with call control interfaces" **40216** may provide necessary call setup and multimedia features in this embodiment, the external Call Control System **40209** is necessary, as are the intervening DDE, OLE or DLL interfaces **40207**, **40212** and **40213**. This embodiment also includes a Video Store and Forward system **40204** and its DDE, OLE or DLL interface **40203**. Finally, the second embodiment adds the internal software system Call Monitor **40202**.

10 As in the first embodiment, the Video Operator Console system **40101** is comprised of a GUI **40102** and a Software System **40103**. However, in addition to the Scheduling system **40104**, the Recording and Playback system **40105** and the Call System Interface **40106**, the software system in the second embodiment includes the MCU control **40201** and the Call
15 Monitor **40202**.

The Scheduling system **40104** and associated external systems **40108**, **40111**, **40114** and **40115** are identical to the those in the first embodiment, pictured in Figure **97** and described above.

20

The internal MCU control **40201** communicates via a DDE, OLE or DLL interface **40206** with the external MCU Control System **40208** to manage resources and features specific to various different MCU systems. The MCU Control System **40208** communicates either via a ConferenceTalk interface
25 **40211** with the VideoServer MCS **40215** or via another vendor-specific interface **40210** with some Other MCU vendors' MCU **40214**.

The Recording and Playback system **40105** communicates via DDE, OLE or DLL interfaces **40109**, **40203** with both the Storage and Retrieval system
30 **40205** and the Video Store and Forward system **40204**. The Storage and Retrieval system **40205** and Video Store and Forward system **40204** communicate via another DDE, OLE or DLL interface **40207** with the Call

Control System **40209**. The Call Control System **40209** communicates via another DDE, OLE or DLL interface **40212** with a uni-directional H.320 recorder **40116** and a uni-directional H.320 playback device **40117**.

5 Conference calls recorded by transmitting the digitized audio and video signals from the Video Operator Console **40101** through the Storage and Retrieval system **40205** and Call Control System **40209** to the H.320 recorder **40116**. Conference calls are played back by retrieving a previously recorded conference call from disk storage and transmitting the audio and video signals from the H.320 playback device **40117** through the Call
10 Control System **40209** and Storage and Retrieval system **40205** to the Video Operator Console **40101**. The Video Store and Forward system **40204** operates in a manner similar to the Storage and Retrieval system **40205**, communicating between the Recording and Playback system **40105** and the Call Control System **40209**.

15 The call monitor **40202** monitors the state of calls and connections by regularly polling the Call System Interface **40106** within the Video Operator Console Software System **40103**. The Call System Interface **40106** communicates via a DDE, OLE or DLL interface **40207** with the Call Control
20 System **40209** to manage call data, including switching functions such as dial, hold, etc., translating between the Video Operator Console **40101** internal data structures and the Call Control System **40209** data. The Call Control System, in turn, manages either the Incite MCP **40113** or Other programs with call control interfaces **40216**.

25 The Media Control system **40107** communicates via a DDE, OLE or DLL interface with the Call Control System **40209**, which communicates via a DDE interface **40110** with the Incite MCP application **40113** or with Other programs with call control interfaces **40216**. The Incite MCP application
30 **40113** provides all necessary call setup features and multimedia features such as video window placement and audio control either directly through a DDE interface **40110** to the internal Media Control system **40102** or via the

-286-

Call Control System **40209**. If Other programs with call control interfaces **40216** are used to provide call setup and multimedia features, they communicated with the Media Control system **40107** via the Call Control System **40209**.

5

C. Video Conference Call Flow

Figure **99** shows how a video conference call initiated by the video operator is connected through the system pictured in Figure **96**. In the first step, illustrated by call flow path **40301**, the video operator initiates a call from the Video Operator Terminal **40001** through the MM Hub **40003** to the BONDING Server **40006**, where the BONDING Server **40006** converts the call to a BONDING call. In the second step, illustrated by call flow path **40302**, the BONDING Server **40006** transmits the BONDING call through the MM Hub **40003** once again, through a WAN Hub **40004**, through MCI **40008**, and to the Client Terminal **40007**. This step is repeated for each Client Terminal **40007** that will participate in the video conference. In the third step, illustrated by call flow path **40303**, the video operator initiates a call from the Video Operator Terminal **40001** through the MM Hub **40003**, through a WAN Hub **40004**, through MCI **40008**, and to the MCU **40005**. In the fourth step, illustrated by call flow path **40304**, the video operator uses the Video Operator Terminal **40001** to bridge the connections to the Client Terminal **40007** and MCU **40005**. Each time the video operator calls a conference call client at its Client Terminal **40007**, the MCU's ANI for the particular conference site is passed in the Calling Party Field to identify each client participating in the conference call with the correct conference site. When the MCU is called, the clients' ANI are passed. The MCU can then identify the correct conference site for each call.

In an alternate embodiment, the client initiates a BONDING call from the Client Terminal **40007** through MCI **40005**, through a WAN Hub **40004**, through the MM Hub **40003**, through the BONDING Server **40006**, and

30

-287-

through the MM Hub **40003** once again to the Video Operator Terminal **40001**. The video operator then places a call to the MCU as illustrated in call flow path **40303** and finally bridges the two calls as illustrated in call flow path **40304**. To determine the correct conference site for the client-initiated call, the initiating client's ANI is passed to the MCU when the connection is made by the video operator.

While a conference call is in progress, the video operator monitors each of the calls from the Video Operator Terminal **40001**. Functions of the video operator include monitoring which calls remain connected, reconnecting disconnected calls, adding new clients to the conference, or joining the conference to inform the clients regarding conference status.

All calls are disconnected to end a conference, and the video operator shared database [**40214** in Figure **98**] reflects an updated conference schedule.

D. Video Operator Software System

1. Class Hierarchy

Figure **100** shows the class hierarchy for video operator software system classes. In one embodiment using the Visual C++ programming language, the VOObject **40401** class is extended from the Visual C++ base class CObject. VOObject **40401** is a Superclass to all classes of objects in the internal software system for the video operator console system, such that all objects in the internal software system inherit attributes from VOObject **40401**.

VOOperator **40402** is an assembly class associated with one VOSchedule **40403** Part-1 Class object and one VOUserPreferences **40404** Part-2 Class object, such that exactly one VOSchedule **40403** object and exactly one VOUserPreferences **40404** object are associated with each VOOperator

40402 object. VOSchedule **40403**, in turn, is an Assembly Class associated with zero or more VOSchedulable **40405** Part-1 Class objects, such that any number of VOSchedulable **40405** objects may be associated with each VOSchedule **40403** object.

5

VOSchedulable **40405** is a Superclass to the VOConference **40406** Subclass-1 and the VOPlaybackSession **40407** Subclass-2, such that the VOConference **40406** object and the VOPlaybackSession **40407** object inherit attributes from the VOSchedulable **40405** object. VOConference

10

40406 is an Assembly Class associated with two or more VOConnection **40412** Part-1 Class objects and zero or one VOPlaybackCall **40415** Part-2 Class objects, such that at least two VOConnection **40412** objects and possibly one VOPlaybackCall **40415** object are associated with each

15

VOConference **40406** object. VOPlaybackSession **40407** is an Assembly Class associated with one VOPlaybackCall **40415** Part-1 Class object, such that exactly one VOPlaybackCall **40415** object is associated with each VOPlaybackSession **40407** object.

VOCallObjMgr **40408** is an Assembly Class for zero or more VOCall **40410** Part-1 Class objects, such that any number of VOCall **40410** objects may be associated with each VOCallObjMgr **40408** object. Similarly,

VOConnObjMgr **40409** is an Assembly Class for zero or more VOConnection **40412** Part-1 Class objects, such that any number of VOConnection **40412** objects may be associated with each VOConnObjMgr **40409** object.

VOConnection **40412** is an Assembly class for two VOCall **40410** Part-1 Class objects, such that exactly two VOCall **40410** objects are associated with each VOConnection **40412** object. VOCall **40410** is a Superclass to

the VOPlaybackCall **40415** Subclass-1, such that VOPlaybackCall **40415** objects inherit attributes from the VOCall **40410** object. VOCall **40410** is

also an Assembly Class associated with two VOSite **40413** Part-1 Class objects, such that exactly two VOSite **40413** objects are associated with each VOCall **40410** object. Finally, the VOCall **40410** class object uses the

VORecorder **40411** class object.

VOSite **40413** is a Superclass to the VOMcuPortSite **40417** Subclass-1, the VOParticipantSite **40418** Subclass-2, and the VOOperatorSite **40419** Subclass-3, such that VOMcuPortSite **40417** objects, VOParticipantSite **40418** objects and VOOperatorSite **40419** objects inherit attributes from the VOSite **40413** object.

VOPlaybackCall **40415** is an Assembly Class associated with one VOMovie **40416**, such that exactly one VOMovie **40416** object is associated with each VOPlaybackCall **40415** object. The VOPlaybackCall **40415** class object also uses the VOPlayer **40414** class object.

VOMessage **40420** object has no associations other than inheriting the attributes of VOObject **40401**, the Superclass to all objects in the internal software system.

2. Class and Object details

a) VOObject

All Internal Software System classes will inherit from the following base class. This base class is extended from the Visual C++ base class *CObject*.

Class	VOObject
Base Class	CObject
Inheritance	public
Type	
Friend Classes	-

(1) Data Types

-290-

```
enum senderType_e { SENDER_INTERNAL, SENDER_SCHEDULE,
SENDER_CONFERENCE, SENDER_CONNECTION, SENDER_CALL,
SENDER_TIMER };
```

```
5 enum messageType_e { MSG_DEBUG, MSG_ERROR, MSG_WARNING, MSG
APPLICATION_ERROR, MSG_STATE_UPDATE };
```

Delivery type flags: DELIVER_MESSAGE_QUEUE, DELIVER_LOG_FILE,
DELIVER_MODAL_DIALOG, DELIVER_MODELESS_DIALOG,

```
10 DELIVER_CONSOLEOUTPUT
```

(2) Attributes

Access Level	Type	Name	Description
static	VOOperator*	m_pVO	video operator pointer
static	VOSchedule*	m_pSchedule	scheduler pointer
static	VOCallObjMgr*	m_pCallOM	Call Object Manager pointer
static	VOConnectionObjMgr*	m_pConnOM	Connection Object Manager pointer
static	VOCallSystem*	m_pCallSys	Call System Interface pointer

(3) Methods

```
15 (a) PostMessage
```

```
virtual PostMessage (messageType_e type, int errCode, CString info="",  
int delivery=(DELIVER_MSG_QUEUE|DELIVER_LOG_FILE),  
senderType_e senderType=SENDER_INTERNAL, void*  
sender=NULL);
```


-291-

(i) Parameters

type The type of message, as defined in the Data Types section

errCode The error or warning code as defined in the application's
resources.

Info Extra textual information to be passed as part of the message.

delivery Preferred method of message delivery. The delivery options are
shown in the Data Types section above. Default method of
delivery is stored in the class member variable m_delivery,
which should be initialized to both
DELIVER_MESSAGE_QUEUE and DELIVER_LOG_FILE
only.

senderType The message sender type, as defined in the Data Types section.

Sender A pointer to the object sending the message, i.e. this

(ii) Description

Use this function to create error, warning, debug, logging and notification
messages. It will create a VOMessage object, which will then perform the
appropriate actions as specified by the delivery flags.

(b) *GetErrorString*

virtual CString GetErrorString (int errorCode);

Return Value: returns a CString object having the error string
corresponding to the error code passed.

errorCode parameter: the error code for which you want the error string.
Error strings are stored as resources.

This function is called to get a textual description corresponding to an error

code.

b) Core Classes

(1) Class List

- 5 Site
 - Participant Site
 - MCU Port Site
 - Video Operator Site
 - Call
- 10 Playback Call
 - Movie
 - Call Object Manager
 - Connection
 - Connection Object Manager
- 15 Message
 - Video Operator

(2) Class Descriptions

(a) Site

- 20 This is a base class from which classes such as the Participant Site and MCU Port Site classes can be derived from. It's main purpose is to function as a data structure containing pertinent information about who or what is taking part in a Call.

Class	VOSite
Base Class	VObject
Inheritance	public
Type	

-293-

Friend Classes -

(i) Data Types

```
enum Bandwidth_e { MULTIRATE, BONDING, AGGREGATED, H0 };
```

5

(ii) Attributes

Access Level	Type	Name	Description
	Cstring	m_name	name of the site
	ID_t	m_ID	Unique site ID
	ID_t	m_locationID	ID for physical location
	Cstring	m_timezone	Time zone
	Cstring	m_dialNumber	Number(s) to dial. See the Call System Interface section for multiple numbers format.
	Bandwidth_e	m_bandwidthUsage	Bandwidth usage
	int	m_maxNumChannels	Maximum number of channels capable
	VOCall*	m_pCall	pointer to Call object that this Site is a part of .
			* Codec or Terminal Type (PictureTel, MCP, etc.)
			* Call Setup Type (dial-in, dial-out)

(b) Participant Site

-294-

Inherits from VOSite base class.

All customers or conference participants will have their information stored in the VO shared database.

5

Class	VOParticipantSite
Base Class	VOSite
Inheritance	public
Type	
Friend Classes	-

Attributes

Access Level	Type	Name	Description
	Cstring	m_coordinatorName	Site coordinator name
	Cstring	m_coordinatorNbr	Site coordinator telephone number
	ID_t	m_companyID	ID of Company this Site belongs to
	VOMCUPortSite*	m_pMCUPort	MCU Port Site that is to be associated with in a Connection object

10

(c) *MCU Port Site*

Inherits from VOSite base class.

All conferences take place on an MCU. Each Participant Site needs to

15 connect with a logical "port" on an MCU.

-295-

Class VOMcuPortSite
 Base Class VOSite
 Inheritance public
 Type
 Friend Classes -

Attributes

Access Level	Type	Name	Description
	ID_t	m_mcuID	ID to identify the MCU
	VOParticipantSite*	m_pParticipant	Participant Site that is to be associated with in a Connection object

5

(d) *Video Operator Site*

Inherits from VOSite base class.

All calls will have the Video Operator Site as one of the sites in a point-to-point call. This structure contains the real ANI of the video operator.

10

Class VOperatorSite
 Base Class VOSite
 Inheritance public
 Type
 Friend Classes -

Attributes

Access	Type	Name	Description
--------	------	------	-------------

-296-

Level			
	ID_t	m_operatorID	Operator's ID
	CString	m_voicePhone	Operator's voice phone number
	ID_t	m_groupID	Operator's Group ID
	ID_t	m_supervisorID	Supervisor's ID
	CObList	m_Calls	list of Call objects that this Site is a part of

(e) *Call*

A Call is defined as a full duplex H.320 stream between two sites. In all Calls, the Video Operator Site will be one of the sites. A Joined pair of Calls is called a Connection.

Class VOCall
 Base Class VOObject
 Inheritance public
 Type
 Friend Classes -

(i) Data Types

enum StateCall_e { ERROR, INACTIVE, INCOMING, DIALING, ACTIVE, DISCONNECTED, HELD, lastCallStates};
 enum callOperation_e { ERROR, DIAL, ANSWER, HOLD, PICKUP, DISCONNECT, HANGUP, lastCallOperations }

(ii) Attributes

Access	Type	Name	Description
--------	------	------	-------------

-297-

Level			
	ID_t	m_ID	call ID
	VOSite*	m_pSite	other end of a call site (Participant, MCU Port or unknown)
	VOOperatorSite*	m_pOperatorSite	Operator site
	boolean	m_operatorInitiated	TRUE if the call is initiated by the operator (default)
	CTime	m_startTime	the actual time when the call became active
	boolean	m_expectHangup	flag that helps determine whether a Hangup is expected or not.
	StateCall_e	m_state	state of the call
	StateCall_e [nCallStates] [nCallOperations]	m_transitionTable	state transition table
	VORecorder*	m_pRecorder	recorder object for call
	VOConnection*	m_pConnection	pointer to Connection object this call belongs to.

(iii) Methods

-298-

Disconnection(); is called when the other end of the line hangs up or the line goes dead. The member variable `m_expectHangup` should be `FALSE`. Otherwise, the Call Object Manager's `Hangup()` operation would have been called.

5

Reset(); resets the call state to an inactive state

RecordingStart(); starts recording the H.320 input pipe of the Call.

10 **RecordingStop();** stops the recording of the Call.

setState(callOperation_e operation);

operation parameter: indicates an operation that has been performed which will result in a change of state

15

Operations that affect the state of the Call should call the **setState** function after the operation has been performed. This function will change the state of the Call by referencing the current state and the operation in the state-transition table. A `VOMessage` object will be created, with a type of

20 `STATUS_UPDATE` and sent to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

(f) *Playback Call*

25 Inherits from `VOCall` base class.

In this special case of a Call, the Video Operator audio and video output is replaced with the H.320 stream from the playback of a movie by the Video Operator Storage and Playback external system component.

30

-299-

Class VOPlaybackCall
 Base Class VOCall
 Inheritance public
 Type
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
	VOMovie*	m_pMovie	the movie object that will be played
	VOPlayer*	m_pPlayer	Player object that performs the playback

5

(ii) Methods

PlaybackStart(); starts playback

PlaybackStop(); stops playback

10

(g) *Movie*

A Movie is a recording of an H.320 Call. For Phase 1, the Video Operator Storage and Playback System manages files and H.320 data streams for recording and playback of movies, as well as storage and retrieval.

Class VOMovie
 Base Class VOObject
 Inheritance public
 Type

-300-

Friend Classes -

Attributes

Access Level	Type	Name	Description
public	ID_t	m_movieID	movie ID
public	CString	m_description	movie description

5

(h) Call Object Manager

By having a Call Object Manager to perform the construction and destruction of Call objects, a list of all calls on the video operator's machine can be maintained. This includes calls that are not part of any Conference or Playback Sessions, including incoming calls and general purpose dial-out calls. Operations that affect a Call but do not create or destroy it can be performed by the Call object itself.

Class VCallObjManager
 Base Class VObject
 Inheritance public
 Type
 Friend -
 Classes

15

(i) Attributes

Access Level	Type	Name	Description

-301-

	int	m_numChannels	total number of unused channels
	int	m_numActive	total number of active channels
	CMapStringToOb	m_callList	list of calls

(ii) Methods

Dial();5 **Dial(VOCall* pCalling);**

pCalling parameter: If not NULL, this pointer will be used for the Call object. This is necessary when creating or re-using a Call object that is in an inactive or disconnected state.

10 Dial performs dial out. The number(s) to Dial are in the m_pSite Call member structure.

Answer();**Answer(VOCall* pIncoming);**

15 pIncoming parameter: If not NULL, this pointer will be used for the Call object. This is necessary when creating or re-using a Call object that is in an inactive or disconnected state.

Answer answers an incoming call.

20

Hangup(VOCall* pCall);

pCall parameter: pointer to the call

Hangup hangs up the call pointed to by pCall

25

Hold(VOCall* pCall);

-302-

pCall parameter: pointer to the call

Hold puts the call pointed to on hold.

5 **VOCall* CallCreate();**

VOCall* CallCreate creates a Call object.

VOPlaybackCall* PlaybackCallCreate();

VOPlaybackCall* PlaybackCallCreate() creates a Playback Call object.

10

VOCall* GetCallPtr(ID_t idCall);

idCall parameter: call ID

VOCall* GetCallPtr gets the pointer to the call object identified by idCall

15

(i) *Connection*

A Connection is defined as a pair of Call objects that maintain a Join state, and each Call has the Video Operator Site as a common point for the Join to be implemented.

20

Class	VOConnection
Base Class	VOObject
Inheritance	public
Type	
Friend Classes	-

(i) *Data Types*

enum StateConnection_e { ERROR, UNJOINED, JOINED, BROKEN,

25 lastConnectionStates };

-303-

```
enum ConnectionOperation_e { ERROR, JOIN, UNJOIN, BREAK, RESET,
lastConnectionOperations };
```

(ii) Attributes

Access Level	Type	Name	Description
	VOCall*	m_pParticipantCall	pointer to the Participant Call
	VOCall*	m_pMCUPortCall	pointer to the MCU Port Call
	VOParticipantSite*	m_pParticipantSite	pointer to the Participant Site
	VOMCUSite*	m_pMCUPortSite	pointer to the MCU Port Site
	CTime	m_joinTime	time of join
	VOMovie*	m_pMovie	movie pointer for recording or playback
	boolean	m_expectBreak	flag that helps determine whether a Break is expected or not.
	StateConnection_e	m_state	state of the connection
	StateConnection_e [nConnectionStates] [nConnectionOps]	m_transitionTable	state transition table
	VOConference*	m_pConference	pointer to the Conference that

-304-

			this Connection is a part of.
--	--	--	----------------------------------

(iii) Methods

Join(); joins the Participant and MCU Port Calls.

- 5 **Unjoin();** unjoins the Participant and MCU Port Calls.

SetParticipantCall(VOCall* participantCall);

participantCall parameter: pointer to a Call object

- 10 SetParticipantCall sets the Call to be the Participant Call. This is useful when managing unknown incoming calls or for last minute participant substitution.

SetMCUPortCall(VOCall* mcuPortCall);

- 15 mcuPortCall parameter: pointer to a Call

SetMCUPortCall sets the Call to be the MCU Port Call. This is useful when managing unknown incoming calls or for last minute call site substitution.

- 20 **DoParticipantCall();** calls the Participant Site and sets it as the Participant Call.

DoMCUPortCall(); calls the MCU Port Site and sets it as the MCU Port Call.

- 25 **setState (ConnectionOperation_e operation);**

operation parameter: the operation that has been performed which will result in a change of state.

Operations that affect the state of the Connection should call the setState

-305-

function after the operation has been performed. This function will change the state of the Connection by referencing the current state and the operation in the state-transition table. A VOMessage object will be created, with a type of STATUS_UPDATE and sent to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

protected Break(); is called when a Joined Connection becomes Un-joined. If the member variable m_expectBreak is FALSE then one of the Calls must have unexpectedly been disconnected. Otherwise, the Connection's Unjoin() operation would have been called.

protected Reset (); resets the state of the Connection to UNJOINED.

(j) *Connection Object Manager*

Similarly with the Call Object Manager, a list of all Connections in operation on the video operator's machine must be maintained. All operations that result in the creation or deletion of a Connection must use the Connection Object Manager.

Class	VOConnectionObjMgr
Base Class	VOObject
Inheritance	public
Type	
Friend Classes	-

(i) *Attributes*

Access Level	Type	Name	Description

-306-

	CMapStringToOb	m_connectionsList	list of all connections
	int	m_numJoined	number of joined connections

(ii) Methods

VOConnection* Create();

5 Return Value: pointer to Connection object

VOConnection* Create creates a new Connection object and adds it to the list.

10 **Remove (VOConnection* oldConnection);**

oldConnection parameter: connection object to be removed

Return Value: returns TRUE if operation successful.

15 Remove deletes a Connection object and removes it from the list.

VOConnection* GetConnectionPtr(ID_t idConnection);

Return Value: a pointer to the connection object

20 idConnection parameter: ID of the Connection

VOConnection* GetConnectionPtr returns the pointer to a Connection object identified by its ID.

25

(k) Message

All one-way communication from the Internal System Software to the rest of

-307-

the Video Operator application, i.e. the Graphical User Interface, is sent as messages that get placed on the Application Queue. The function to create and post a Message is in the base class VObject, which all Internal System Software classes inherit from. All run-time errors or debugging information is put into a Message object, and posted to the application queue so that an appropriate object will process it according to its type and severity. Therefore all class functions that do not return a specific type will post a Message if something goes wrong, e.g. out of memory, or debugging information to be displayed by the GUI or logged to a file.

Class	VOMessage
Base Class	VObject
Inheritance	public
Type	
Friend Classes	-

(i) Data Types

```

15  enum senderType_e { INTERNAL, SCHEDULE, CONFERENCE,
    CONNECTION, CALL, TIMER };
    enum messageType_e { DEBUG, ERROR, WARNING, APPLICATION_ERROR,
    STATE_UPDATE };

20  Delivery type flags: DELIVER_MESSAGE_QUEUE, DELIVER_LOG_FILE,
    DELIVER_MODAL_DIALOG, DELIVER_MODELESS_DIALOG,
    DELIVER_CONSOLEOUTPUT

```

25

(ii) Attributes

Access Level	Type	Name	Description
	int	m_errorCode	error code
	int	m_delivery	flags for preferred message delivery when posting.
	senderType_e	m_senderType	sender type
	VOObject*	m_pObject	pointer to the sender
	messageType_e	m_messageType	type of the message
	CString	m_info	message info
			* priority of message or error
			* severity of message or error

(iii) Methods

Post(); posts a message to the application message queue

5

private static AppendLog();

Return Value: returns TRUE if the operation is successful.

This method is called by VOObject::PostMessage() when the flag for

10 DELIVER_LOG_FILE is set.

(l) Video Operator

Generally there will be only one Video Operator per machine. Each Video Operator has a Schedule, and a list of customer Participant Sites to manage.

15 The Call Object Manager and Connection Object Manager are also part of the Video Operator.

-309-

Class	VOOperator
Base Class	VOObject
Inheritance	public
Type	
Friend Classes	-

(i) Attributes

Access Level	Type	Name	Description
	ID_t	m_operatorID	operatorID
	VOSchedule	m_schedule	schedule for the current operator
	CObList	m_MCUlist	list of MCU objects
	CObList	m_operatorSites	Operator's site(s)
static	VOUserPreferences	m_userPreferences	default application user preferences

5

(ii) Methods

protected ScheduleStart(); initiates the schedule for the video operator.

protected CallObjMgrStart(); initiates the call object manager.

10 **protected ConnectionObjMgrStart();** initiates the connection object manager.

protected CallSystemInterfaceStart(); initiates the Call System Interface.

15

(m) User Preferences

-310-

The Video Operator Console application will have a set of default application preferences which may be modified and saved. The values of these variables are taken from the following sources, in order of increasing preference: hard-coded default values, saved VO.INI file, command-line invocation arguments, GUI entry and run-time modifications saved to VO.INI file.

Class VOUserPreferences
 Base Class VObject
 Inheritance public
 Type
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
	ID_t	m_operatorID	default operatorID

(ii) Methods

SavePrefs(); saves all values to VO.INI.

LoadPrefs(); loads all values from VO.INI.

(n) MCU

All MCU Port Sites correspond to a particular MCU. This class is used for MCU Port Site storage only. For Phase 2, MCU specific operations and interfaces would be implemented here.

Class VOMCU
 Base Class VObject

-311-

Inheritance public
 Type
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
	ID_t	m_mcuID	ID of the MCU
	CObList	m_portList	List of MCU Port Site objects

5

(ii) Methods

VOMCUPortSite* GetPortPtr(ID_t idPort);

Return Value: a pointer to the MCU Port Site object.

IdPort parameter: ID of the MCU Port Site

- 10 VOMCUPortSite* GetPortPtr returns the pointer to a MCU Port Site object identified by its ID.

VOMCUPortSite* CreatePort();

Return Value: a pointer to a new MCU Port Site object

15

VOMCUPortSite* CreatePort returns the pointer to a newly created MCU Port Site object identified by its ID.

(3) State Variable Transition Diagrams for Core
 Classes

20

Figure **101** shows a state transition diagram illustrating the state changes

that may occur in the VOCall object's m_state variable ("state variable"). The state variable starts **40501** in Inactive **40502** state.

If the VOCall object receives a Dial **40503** input while in Inactive **40502** state, the state variable changes to Dialing **40504** state. In the Dialing **40504** state, the state variable changes to Inactive **40502** state upon receiving a Busy **40505** input or to Active **40507** state upon receiving an Answer **40506** input. In the Active **40507** state, the state variable changes to Held **40510** state upon receiving a Hold **40509** input, to Disconnected **40515** state upon receiving a Disconnection **40514** input, or to Inactive **40502** state upon receiving a Hangup **40508** input. In the Held **40510** state, the state variable changes to Active **40507** state upon receiving a Pickup **40511** input, to Disconnected **40515** state upon receiving a Disconnection **40513** input, or to Inactive **40502** state upon receiving a Hangup **40512** input. In the Disconnected **40515** state, the state variable changes to Inactive **40502** state upon receiving a Reset **40516** input.

If the VOCall object receives an Incoming Call **40517** input while in Inactive **40502** state, the state variable changes to Incoming **40518** state. In the Incoming **40518** state, the state variable changes to Inactive **40502** state upon receiving a Reject **40520** input or to Active **40507** state upon receiving an Answer **40519** input.

Figure **102** shows a state transition diagram illustrating the state changes that may occur in the VOConnection object's m_state variable ("state variable"). The state variable starts **40601** in Unjoined **40602** state. In the Unjoined **40602** state, the state variable changes to Joined **40604** state upon receiving a Join **40603** input. In the Joined **40604** state, the state variable changes to Unjoined **40602** state upon receiving an Unjoin **40605** input or to Broken **40607** state upon receiving a Break **40606** input. In the Broken **40607** state, the state variable changes to Joined **40604** state upon receiving a Join **40608** input.

c) Scheduling System Classes

(1) Class List

Playback Session

Conference

5 Schedule

Schedulable

(2) Class Descriptions

(a) *Playback Session*

10 Like Conferences, Playback Sessions need to be scheduled. A Call is made with a Participant Site and the Video Operator Site. The Video Operator Storage and Playback external component system will playback a scheduled and pre-selected movie, replacing the AV output to the Participant Site. No MCU is used for a Playback Session, and only one Participant Site is involved in one embodiment.

15

Class	VOPlaybackSession
Base Class	VOSchedulable
Inheritance	public
Type	
Friend	-
Classes	

(i) Data Types

20 enum StatePlaybackSession_e { ERROR, INACTIVE, SETUP, ACTIVE, ENDING, FINISHED, lastPBSessionStates };

enum playbackSessionOperation_e { ERROR, PREPARE, START, CLOSE, FINISH, lastPBSessionOperations};

-314-

(ii) Attributes

Access Level	Type	Name	Description
public	ID_t	m_ID	ID assigned when a reservation is made for the session
public	CString	m_name	a short name for the session
public	CString	m_description	a brief description
public	CTime	m_startTime	start time
public	CTimeSpan	m_duration	the duration of the playback session
public	int	m_xferRate	The data transfer rate (number of channels)
protected	VOPlaybackCall*	m_playbackCall	the playback call object
protected	StatePlaybackSession_e	m_state	state of playback session
protected	StatePlaybackSession_e [lastPBSessionStates]	m_transitionTable	The state transition

-315-

	[lastPBSessionOps]		table
--	--------------------	--	-------

(iii) Methods

public boolean Setup();

Return Value: returns TRUE if operation successful.

5

public boolean Setup() sets up the Playback Call by calling the Participant Site and initialize a VOPlayer object. This function may be called by the Scheduler.

10 **Public boolean Start();**

Return Value: returns TRUE if operation successful.

Public boolean Start starts the Player to play to the Playback Call. This function may be called by the Scheduler.

15

Public boolean Close();

Return Value: returns TRUE if operation successful.

Public boolean Close sends messages to the Video Operator and maybe the Participant that the Playback Session will end soon.

20

Public boolean Finish();

Return Value: returns TRUE if operation successful.

25 Public boolean Finish stops the Player and Hangup the Playback Call. This function may be called by the Scheduler.

public StatePlaybackSession_e StateGet();

Return Value: returns the playback session's state.

30

-316-

Use the public StatePlaybackSession_e StateGet; function to find out the state of the Playback Session.

protected boolean StateSet(playbackSessionOperation_e operation);

5 Return Value: returns TRUE if operation successful.

operation parameter: the operation that has been performed which will result in a change of state

10 Operations that affect the state of the Playback Session should call the protected boolean StateSet function after the operation has been performed. This function will change the state of the Playback Session by referencing the current state and the operation in the state-transition table. A VOMessage object will be created, with a type of STATUS_UPDATE and sent
15 to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

(b) Conference

The main function of the Video Operator is to manage conferences. The
20 scheduler system creates the Conference objects, which in turn create a list of Connections (or Participant-MCU Port Site Call pairs). In the special case of a movie being played back to a conference, an extra call is made to an MCU Port and the movie is played back to the MCU in a similar way as a Playback Session. This of course requires an extra MCU Port site to be
25 available, and must be scheduled before the start of the conference.

Class	VOConference
Base Class	VOSchedulabl e
Inheritance	public

-317-

Type

Friend Classes -

(i) Data Types

```
enum conferenceMode_e { CONTINUOUS_PRESENCE, VOICE_ACTIVATED,
```

```
5 LECTURE, DIRECTOR_CONTROL };
```

```
enum StateConference_e { ERROR, INACTIVE, SETUP, ACTIVE, ENDING,  
FINISHED, lastConferenceStates};
```

```
enum conferenceOperation_e { ERROR, PREPARE, START, CLOSE, FINISH,  
lastConferenceOperations};
```

10

(ii) Attributes

Access Level	Type	Name	Description
	ID_t	m_ID	Conference ID given when the reservation is made
	CString	m_name	name for conference
	CString	m_description	brief description
	CString	m_timeZone	time zone
	CTime	m_startTime	start time of the conference
	CTimeSpan	m_duration	duration of the conference
	int	m_transferRate	transfer rate

-318-

	int	m_numActiveConns	number of active connections
	conferenceMode_e	m_mode	conference mode
	boolean	m_recordingScheduled	TRUE if this conference is to be recorded
	CObList	m_connectionsList	List to store the connection objects
	CMapStringToObj	m_participantSiteList	List of participant sites
	VOPlaybackCall	m_playbackCall	If there is a playback in the conference, this is valid
	StateConference_e	m_state	current state of conference
	StateConference_e [lastConferenceStates] [lastConferenceOps]	m_transitionTable	state transition table
			*Cal l Set up Type
			*Audio Prot

-319-

			ocol
			*Vid
			eo
			Prot
			ocol
			*Mu
			lti
			MC
			U
			Con
			fere
			nce
			*H.
			243
			Cha
			ir
			Con
			trol
			&
			pas
			swo
			rd

(iii) Methods

public boolean Setup();

5 Return Value: returns TRUE if operation successful.

public boolean Setup sets up each Connection in the connection list (and the Playback Call if required) by calling each Participant Site and MCU Port Site as appropriate, and perform the Join operations to create the

-320-

Connections. This function may be called by the Scheduler.

Public boolean Start();

Return Value: returns TRUE if operation successful.

5

Public boolean Start starts the Conference. This function may be called by the Scheduler.

Public boolean End();

10 Return Value: returns TRUE if operation successful.

Public boolean End starts tearing down the Connections in the conference or issues warnings that the conference will end soon. This function may be called by the Scheduler.

15

Public boolean Finish();

Return Value: returns TRUE if operation successful.

20 Public boolean Finish stops the Conference and hangs up all Calls in the Conference. This function may be called by the Scheduler.

public StateConference_e StateGet();

Return Value: returns the Conference state

25 Use the public StateConference_e StateGet function to find out the state of the Conference.

protected boolean StateSet(conferenceOperation_e operation);

Return Value: returns TRUE if operation successful.

30 operation parameter: the operation that has been performed which will result in a change of state

-321-

Operations that affect the state of the Conference should call the protected boolean StateSet function after the operation has been performed. This function will change the state of the Conference by referencing the current state and the operation in the state-transition table. A VOMessage object will be created, with a type of STATUS_UPDATE and sent to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

(c) *Schedule*

10 The Scheduling System maintains a list of Conferences and Playback Sessions. Each Conference and Playback Session is created at a particular time interval before its starting time. The Schedule in memory and the Schedule stored in the Video Operator Shared Database for the current Video Operator should always be synchronized.

15

Class	VOSchedule
Base Class	VOObject
Inheritance	public
Type	
Friend Classes	-

(i) *Attributes*

Access Level	Type	Name	Description
	ID_t	m_operatorID	responsible operator ID
	CMapStringToObj	m_schedItems	list of schedulable objects (Conferences and Playback Sessions)
	CMapWordToObj	m_schedAlar	list of alarms currently set

-322-

		ms	for operations on schedulable objects (construction and deletion)
--	--	----	---

(ii) Methods

SynchWithDb(); synchronizes with the VO shared database for the schedule.

5

AddSchedulable(VOSchedulable* pSchedulable);

pSchedulable parameter: pointer to schedulable object to be added to list

AddSchedulable adds a Schedulable object to the list

10

DeleteSchedulable(ID_t aSchedulable);

aSchedulable parameter: schedulable object to be removed from list

15

DeleteSchedulable deletes a Schedulable object and remove from list.

(d) *Schedulable*

Items or Objects that are schedulable in Phase 1 are Conferences and Playback Sessions. This class allows us to create a schedule for any type of event.

20

Class	VOSchedulable
Base Class	VOObject
Inheritance	public
Type	
Friend Classes	-

-323-

(i) Attributes

Access Level	Type	Name	Description
	ID_t	m_requestor	ID of requestor
	Ctime	m_startTime	scheduled starting time
	CtimeSpan	m_duration	scheduled duration of event
	Ctime	m_endTime	scheduled end time of event
	MMRESULT	m_alarmID	ID of alarm currently set

(ii) Methods

- 5 **public SetAlarm(Ctime time, LPTIMECALLBACK func);**
time parameter: time for alarm to be triggered
func parameter: pointer to callback function when alarm is triggered
Return Value: returns TRUE if operation successful.
- 10 public SetAlarm sets an alarm to be triggered at a specified time. When the alarm is triggered, the callback function will be called. This is useful for time dependant events such as 15 minutes before a Conference starts, 5 minutes before a Conference ends, and 30 minutes after a Conference has finished.
- 15 **public KillAlarm();**
Return Value: returns TRUE if operation successful.
- 20 public KillAlarm kills the last alarm that has been set by SetAlarm(). This would be used in the case of aborting a Conference, etc.

-324-

(3) State Variable Transition Diagram for
Schedule System Classes

Figure **103** shows a state transition diagram illustrating the state changes that may occur in the VOConference object's m_state variable ("state variable"). The state variable starts **40701** in Inactive **40702** state. In the
5 Inactive **40702** state, the state variable changes to ConnectionSetup **40704** state upon receiving a "15 minutes before scheduled time" **40703** input. In the ConnectionSetup **40704** state, the state variable changes to Active
10 **40706** state upon receiving a Start Conference **40705** input. In the Active **40706** state, the state variable remains in Active **40706** state upon receiving an Extend Conference **40707** input or changes to Ending **40707** state upon receiving a CloseConference (Proper Termination) **40708** input. In the Ending **40707** state, the state variable changes to Finished **40711** state upon receiving a Finish **40710** input.

15

d) Recording and Playback Classes

(1) Class List

Recorder
Player

20

(2) Class Details

(a) Recorder

A recorder communicates with whatever external components performs the actual movie creation and recording of the input pipe of a Call. This external component is known as the Video Operator Storage and Playback
25 system.

Class	VORecorder
Base Class	VOObject

-325-

Inheritance public
 Type
 Friend Classes -

(i) Data Types

enum StateRecorder_e { ERROR, IDLE, RECORDING, PAUSED, FINISHED,
 5 lastRecorderStates};
 enum recorderOperation_e { ERROR, BEGIN, PAUSE, RESUME, STOP,
 lastRecorderOps }

(ii) Attributes

Access level	Type	Name	Description
	VOMovie*	m_movie	Movie
	VOCall*	m_pCall	Call pointer (for recording)
	Cstring	m_info	Participant and Conference Names
	Ctime	m_startTime	Start Time
	Ctime	m_endTime	End time
	CtimeSpan	m_duration	Total recorded time
	StateRecorder_e	m_state	State
	StateRecorder_e [lastRecorderStates] [lastRecorderOps]	m_transitionTable	state transition table
			*VSF Object
			*Recording Mode

-326-

(iii) Methods

InitMovie(); VOSP initializes a recording. This will tell the VOSP to prepare to record.

5 **start();** VOSP starts a recording.

stop(); VOSP stops a recording.

setState(recorderOperation_e operation);

10

operation parameter: the operation that has been performed which will result in a change of state.

Operations that affect the state of the Recorder should call the **setState** function after the operation has been performed. This function will change the state of the Recorder by referencing the current state and the operation in the state-transition table. A VOMessage object will be created, with a type of STATUS_UPDATE and sent to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

20

(b) *Player*

A Player communicates with whatever external component performs the actual playback of a movie to the output pipe of a Call. For Phase 1, this external component is known as the Video Operator Storage and Playback system.

25

Class	VOPlayer
Base Class	VObject
Inheritance	public

-327-

Type

Friend Classes -

(i) Data Types

```
enum StatePlayer_e    { ERROR, IDLE, PLAYING, PAUSED, FINISHED,
nPlayerStates};
```

```
5 enum playerOperation_e    { ERROR, BEGIN, PAUSE, RESUME, STOP,
RESET, nPlayerOps }
```

(ii) Attributes

Access level	Type	Name	Description
	VOMovie*	m_pMovie	Movie
	VOCall*	m_pCall	Call pointer (for playback)
	Cstring	m_info	Participant and Conference Names
	Ctime	m_startTime	Start and End Time
	Ctime	m_endTime	
	CTimeSpan	m_duration	Total playback time
	StatePlayer_e	m_state	State
	StatePlayer_e [nPlayerStates] [nPlayerOps]	m_transitionTable	state transition table
			*VSF Object
			*Playback Mode

10

(iii) Methods

```
public InitMovie();
```

Return Value: returns TRUE if operation successful.

-328-

public InitMovie VOSP initializes playback. This will tell the VOSP to prepare for playback.

5 **public Start();**

Return Value: returns TRUE if operation successful.

public Start VOSP starts playback.

10 **public Stop();**

Return Value: returns TRUE if operation successful.

public Stop VOSP stops playback.

15 **setstate(playerOperation_e operation);**

Return Value: returns TRUE if operation successful.

operation parameter: the operation that has been performed which will result in a change of state.

20

Operations that affect the state of the Player should call the setstate function after the operation has been performed. This function will change the state of the Player by referencing the current state and the operation in the state-transition table. A VOMessage object will be created, with a type of
25 STATUS_UPDATE and sent to the application queue. The GUI and any other component that reads the application queue will therefore be informed of the status update.

(3) State Transition Diagrams for Recording and
30 Playback Classes

Figure 104 shows a state transition diagram illustrating the state changes

that may occur in the VORecorder object's m_state variable ("state variable"). The state variable starts **40801** in Idle **40802** state. In the Idle **40802** state, the state variable changes to Recording **40804** state upon receiving a Begin Recording **40803** input. In the Recording **40804** state, the state variable changes to Paused **40806** state upon receiving a Pause **40805** input or to Finished **40810** state upon receiving a Stop **40808** input. In the Paused **40806** state, the state variable changes to Recording **40804** state upon receiving a Resume **40807** input or to Finished **40810** state upon receiving a Stop **40809** input.

Figure **105** shows a state transition diagram illustrating the state changes that may occur in the VOPlayer object's m_state variable ("state variable"). The state variable starts **40901** in Idle **40902** state. In the Idle **40902** state, the state variable changes to Playing **40904** state upon receiving a Begin Playing **40903** input. In the Playing **40904** state, the state variable changes to Paused **40906** state upon receiving a Pause **40905** input or to Finished **40910** state upon receiving a Stop **40908** input. In the Paused **40906** state, the state variable changes to Playing **40904** state upon receiving a Resume **40907** input or to Finished **40910** state upon receiving a Stop **40909** input. In the Finished **40910** state, the state variable changes to Playing **40904** state upon receiving a Replay **40911** input.

e) Call System Interface Class Description

The Call Control System will manage all calls that a Video Operator can manage. This includes incoming and outgoing H.320 call management and low level operations on a call, such as recording and playback. The Video Operator Application uses its Call System Interface to communicate with the Call Control System external component which manages all calls in a uniform way. This allows the video operator to manage calls that require different external programs, adding an extra codec to the machine, or even managing calls on a remote machine.

-330-

Class VCallSys
 Base Class VObject
 Inheritance public
 Type
 Friend Classes -

(1) Data Types

enum Bandwidth_e { MULTIRATE, BONDING, AGGREGATED, H0 }

5

Q.931 UserInfo for a call using BONDING:

0x00 0x01 0x07 0x44 0x79 0x00 0x00

0 1 7 447-9000

Bonded, 1 number, 7 digits long, 447-9000

10

Q.931 UserInfo for Aggregation:

0x01 0x02 0x07 0x44 0x79 0x00 0x00 0xFF 0x01

1 2 7 447-9000 , 1

Aggregated, 2 numbers, 7 digits long, 447-9000, 447-9001

15

(2) Attributes

Access Level	Type	Name	Description
public	int	m_numCalls	total number of calls available
public	int	m_numConnections	total number of connections available

-331-

(3) Methods

public Dial(Bandwidth_e calltype, CString destination);
public Dial(Bandwidth_e calltype, CString destination, CString
origination);

- 5 Return Value: returns TRUE if operation successful.
calltype parameter: specifies the type of call to make.
destination parameter: specifies the destination number to be dialed.
origination parameter: specifies an origination number to be used, instead
of the real number of the operator's console.

10

public Dial dials out.

public Answer(ID_t call);

call parameter: The Call ID of a Call waiting to be answered.

15

public Answer answers an incoming call.

public Hangup(ID_t call);

Return Value: returns TRUE if operation successful.

20 call parameter: the Call ID of a Call to Hangup

public Hangup hangs up a call.

public Hold(ID_t call);

25 Return Value: returns TRUE if operation successful.

call parameter: the Call ID of a Call to Hold

public Hold puts the call on hold.

30 **public Join(ID_t call1, ID_t call2);**

Return Value: returns TRUE if operation successful.

-332-

call1 parameter: the Call ID of a Call.

call2 parameter: the Call ID of a Call.

public Join joins two Calls.

5

(ID_t connection);

Return Value: returns TRUE if operation successful.

connection parameter: the ID of a Connection to Unjoin

10 public Unjoin un-joins the specified Connection.

public StateCall_e CallStatus(ID_t call);

Return Value: returns the state of a Call

connection parameter: the ID of a Connection to Unjoin

15

public StateCall_e CallStatus reports status of the specified Call.

public StateConnection_e JoinStatus(ID_t connection);

Return Value: returns the state of a Connection

20 connection parameter: the ID of a Connection to Unjoin

public StateConnection_e JoinStatus reports status of the specified Join.

protected LaunchMCP();

25 Return Value: returns TRUE if operation successful.

protected LaunchMCP launches Incite's MCP application.

E. Graphical User Interface Classes

1. Class Hierarchy

Figure **106** shows the class hierarchy for the video operator graphics user interface ("GUI") classes. In general, the video conference operator will perform all the features of the video conferencing operator system described herein by interacting with the video operator console GUI ("console GUI"). The main components of the console GUI are the Main Console Window, Schedule and Connection List Windows, Conference and Connection Windows, a message area, audio and video controls, dialog boxes presenting timely information, and menu items for actions that may be performed infrequently. MCU operations and features will not be implemented in the video operator console GUI, so as to allow different embodiments of the video operator system employing different MCU model types. Vendor-specific MCU operations will be performed by the vendor's software that comes with the MCU application. In one embodiment employing VideoServer's MCS, the MCS Workstation Software can be used to implement features such as conference finish time extension, audio and video blocking, conference director control, etc. This software can run in parallel to the video operator GUI.

Described in object-oriented programming terms, the GUI has a main application object which creates and maintains all the windows and views within. The main window is the VOMainFrame **41009** which is created by the VOConsoleApp **41008**. This mainframe window creates the VOScheduleWnd **41016**, VOAlertWnd **41015**, VOConferenceVw **41014** and the VOVideoWatchVw **41013**. The VOScheduleWnd **41016** and the VOAlertWnd are dockable windows meaning that they can be attached to one of the sides of their parent window. In this case the parent window is the VOMainFrame **41009** window. The dockable windows can also be separated from the border by dragging them away. In such a situation they will act like normal tool windows.

-334-

The function of each class of object can be summarized as follows.

VOConsoleApp **41008** is the main application class, and VOMainFrame **41009** is the main window which contains all the other windows.

- 5 VOScheduleWnd **41016** is a window displaying the operator's schedule, and VOAlertWnd **41015** is a window where the error messages and alerts are displayed. VOChildFrame **41010** is a frame window for the multiple document interface ("MDI") windows. VOChildFrame **41010** will act like the mainframe window for each of the views. VOConferenceFrame **41018**,
10 derived from the VOChildFrame **41010**, is the frame window for the conference view, and VOConferenceVw **41014** is the window displaying the conference information. VOConferenceDoc **41012** is the document class corresponding to the VOConferenceVw **41014**. VOVideoWatchFrame **41017**, derived from the VOChildFrame **41010**, is the frame window for the
15 Video Watch view, and VOVideoWatchVw **41013** is the window displaying the video stream and controls for making calls. VOVideoWatchDoc **41011** is the document class corresponding to the VideoWatch view.

- In one embodiment using Visual C++ as the programming language, CWnd
20 **41001** is a Superclass to the CMDIFrameWnd **41005** Subclass-1, CMDIChildWnd **41006** Subclass-2, CFromView **41007** Subclass-3, and CDialogBar **41002** Subclass-4, such that CMDIFrameWnd **41005** class objects, CMDIChildWnd **41006** class objects, CFromView **41007** class objects, and CDialogBar **41002** class objects inherit attributes from the
25 CWnd **41001** class. CMDIFrameWnd **41005** is a Superclass to VOMainFrame **41009** Subclass-1; CMDIChildWnd **41006** is a Superclass to VOChildFrame **41010** Subclass-1; CFromView **41007** is a Superclass to both VOVideoWatchVw **41013** Subclass-1 and VOConferenceVw **41014** Subclass-2; and CDialogBar **41002** is a Superclass to both VOAlertWnd
30 **41015** Subclass-1 and VOScheduleWnd **41016** Subclass-2. VOChildFrame **41010** is a Superclass to both VOVideoWatchFrame **41017** Subclass-1 and VOConferenceFrame **41018** Subclass-2. CWinApp **41003** is a Superclass

to VOConsoleApp **41008** Subclass-1, and CDocument **41004** is a Superclass to both VOVideoWatchDoc **41011** Subclass-1 and VOConferenceDoc **41012** Subclass-2.

- 5 VOConsoleApp **41008** is an Assembly Class associated with one VOMainFrame **41009** Part-1 Class object, such that exactly one VOMainFrame **41009** object is associated with each VOConsoleApp **41008** object. VOMainFrame **41009** is an Assembly Class associated with one VOVideoWatchFrame **41017** Part-1 Class object, one VOConferenceFrame
- 10 **41018** Part-2 Class object, one VOAlertWnd **41015** Part-3 Class object, and one VOScheduleWnd **41016** Part-4 Class object, such that exactly one VOVideoWatchFrame **41017** object, exactly one VOConferenceFrame **41018** object, exactly one VOAlertWnd **41015** object, and exactly one VOScheduleWnd **41016** object are associated with each VOMainFrame
- 15 **41009** object.

- VOVideoWatchFrame **41017** is an Assembly Class associated with one VOVideoWatchDoc **41011** Part-1 Class object and one VOVideoWatchVw **41013** Part-2 Class object, such that exactly one VOVideoWatchDoc **41011**
- 20 object and exactly one VOVideoWatchVw **41013** object are associated with each VOVideoWatchFrame **41017** object. Each VOVideoWatchDoc **41011** object, extended from the CDocument **41004** class object as discussed above, uses a VOVideoWatchVw **41013** object, extended from the CFormView **41007** class object.

25

- Similarly, VOConferenceFrame **41018** is an Assembly Class associated with one VOConferenceDoc **41012** Part-1 Class object and one VOConferenceVw **41014** Part-2 Class object, such that exactly one VOConferenceDoc **41012** object and exactly one VOConferenceVw **41014** object are associated with
- 30 each VOConferenceFrame **41018** object. VOConferenceDoc **41012** uses VOConferenceVw **41014**.

2. Class and Object details

a) User Interface Classes

(1) Class List

- VOConsoleApp** The main application class
- 5 **VOMainFrame** The main window which has all the other windows
- VOScheduleWnd** Window displaying the operator's schedule
- VOOutputWnd** Window where the error messages and alerts are displayed
- 10 **VOChildFrame** Frame window for the MDI windows. This will act like the mainframe window for each of the views.
- VOConferenceFrame** The frame window for the conference view. This is derived from the VOChildFrame
- VOConferenceVw** The window displaying the conference information
- 15 **VOConferenceDoc** The document class corresponding to the VOConferenceVw
- VOVideoWatchFrame** The frame window for the Video Watch view. This is derived from the VOChildFrame
- VOVideoWatchVw** The window displaying the video stream and controls for making calls.
- 20 **VOVideoWatchDoc** Document class corresponding to the VideoWatch view.

(2) Class Details

(a) VOConsoleApp

Class	VOConsoleApp
Base Class	CWinApp
Inheritance Type	public
Friend Classes	-

-337-

(i) Attributes

Access Level	Type	Name	Description
protected	VOOperator*	m_pOperator	A pointer to the logged in video operator

(ii) Methods

5 **Retcode CreateVideoOperator(CString login, CString password);**

Return Value: returns a non-zero value if successful, zero otherwise.

login parameter: login id for the operator

password parameter: operator's password

10

The Retcode CreateVideoOperator function is initially called during the application instantiation.

Retcode InitializeCallSystemComponents();

15 Return Value: returns a non-zero value if successful, zero otherwise

The Retcode InitializeCallSystemComponents function is initially called during the application initiation, after the creation of the video operator, which makes a local copy of the pointers to the VOCallSystemInterface, VOCallObjMgr and the VOConnectionObjMgr objects, initiated by the

20 internal software system.

void OnGetVOMessage(VOMsg voMsg);

voMsg parameter: the message object passed by the internal software

25 system

-338-

The void OnGetVOMessage function is called when the application receives a message from the internal software system to redirect the message to the appropriate windows. In the initial implementation, the message will be passed on to the VOMainFrame, which interprets the message. Depending on the type of the message it is either displayed in the VOOutputWnd, displayed in a message box, or passed on to the VOConferenceVw and the VOVideoWatch windows.

10

(b) *VOMainFrame*

Class VOMainFrame
 Base Class CFrameWnd
 Inheritance Type public
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
protected	VOOperator*	m_pOperator	A pointer to the logged in video operator
	VOScheduleWnd*	m_pScheduleWnd	A pointer to the schedule window
	VOOutputWnd*	m_pOutputWnd	A pointer to the output window
	VOConferneceVw*	m_pConfVw	A pointer to the conference window. This will be collection if we have multiple conference

-339-

		windows active at the same time.
VOVideoWatchVw *	m_pVideoWatchVw	Pointer to the video watch window.

(ii) Methods

Retcode SynchWithDb();

- 5 Return Value: returns a non-zero value if successful. zero otherwise
 login parameter: login id for the operator
 password parameter: operator's password

The Retcode SynchWithDb function is called if the schedule has changed
 10 and the needs to be synchronized with the database.

Retcode DisplayMessage(VOMsg voMsg);

- Return Value: returns a non-zero successful, zero otherwise
 voMsg parameter: the VOMsg object received from the internal software
 15 system

The Retcode DisplayMessage function displays the content of the voMsg
 object in the output window. Based on the severity, an alert message box is
 also displayed.

20 **void OnConferenceStatusChanged(VOConference* pConference);**

pConference parameter: pointer to the conference object whose status has
 changed

- 25 The void OnConferenceStatusChanged function is called when the status of
 a particular conference has changed.

-340-

(c) *VOScheduleWnd*

Class VOScheduleWnd
 Base Class CDialogBar
 Inheritance Type public
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
protected	VOMainFrame*	m_pMainFrame	A pointer to the Main Frame window
	VOSchedule*	m_pSchedule	pointer to the video operator's schedule

5

(ii) Methods

Retcode DisplaySchedule(BOOL filter = 0);

Return Value: returns a non-zero value if successful. zero otherwise

filter parameter: the filter to be applied for display of the schedule. filter = 0

displays the entire schedule. filter = 1 displays only the active conferences

10 and playback calls

The Retcode DisplaySchedule function is called to display the list of conferences and playback calls in the schedule window.

15 **Retcode DisplayConfSites(VOConference* pConference);**

Return Value: returns a non-zero value if successful. zero otherwise

pConference parameter: pointer to the conference object for which the sites have to be displayed in the sites list box of the schedule window.

20 The Retcode DisplayConfSites function is called to display the list of sites in

-341-

a site list box of the schedule window.

Retcode OnClickScheduledItem();

Return Value: returns a non-zero value if the selection is different from the
5 previous selection. zero otherwise

The Retcode OnClickScheduledItem function is called when the user clicks
on an item in the schedule list box. The initial implementation displays the
corresponding sites in the conference or the site and the movie details in the
10 playback call.

Retcode OnDbClickScheduledItem();

Return Value: returns a non-zero value if a conference window is opened.
zero otherwise
15

The **Retcode OnDbClickScheduledItem** function is called when the user
double clicks on an item in the schedule list box. The initial implementation
creates a new VOConferenceVw for the scheduled item.

20 **Retcode OnClickSite();**

Return Value: returns a non-zero value if the selection is different from the
previous selection. zero otherwise

The Retcode OnClickSite function is called when the user clicks on an item
25 in the site list box of the Schedule window.

(d) *VOOutputWnd*

Class	VOOutputWnd
Base Class	CDialogBar

-342-

Inheritance Type public
 Friend Classes -

(i) Attributes

Access Level	Type	Name	Description
protected	VOMainframe*	m_pMainframe	pointer to the mainframe window

(ii) Methods

5 **Retcode DisplayMessage(CString info, VOMsg* pVoMsg = NULL);**

Return Value: returns a non-zero value if successful. zero otherwise

info parameter: additional information to be displayed

pVoMsg parameter: a pointer to a VOMsg object

- 10 Retcode DisplayMessage displays a message text in the output window. If pVoMsg = NULL, only the info will be displayed.

(e) VOConferenceVw

Class VOConferenceVw
 Base Class CFormView
 Inheritance Type public
 Friend Classes -

15

(i) Attributes

Access Level	Type	Name	Description
protected	VOOperator*	m_pOperator	A pointer to the

-343-

			logged in video operator
	VOMainFrame*	m_pMainframe	A pointer to the mainframe window
	VOVideoWatchVw*	m_pVideoWatchVw	A pointer to the video watch window
	VOOutputWnd*	m_pOutputWnd	pointer to the output window

(ii) Constructor(s)

protected VOConferneceVw();

VOConferenceVw(VOConference* pConference);

5 **VOConferenceVw(VOPlaybackSession* pPbSession);**

pConference parameter: a pointer to the conference object for which the view is to be created.

10 pPbSession parameter: a pointer to the playback session object for which the view is to be created.

The conference view is used to display the information about any conference or a scheduled playback session. This view is created only by the mainframe when the user double clicks on a conference/playback session in the
15 schedule window.

(iii) Methods

(VOConference* pConference);

20 PConference parameter: a pointer to the conference object whose status has changed.

void OnConferenceStatusChanged is called when the conference status has

-344-

changed so that the UI can be updated accordingly.

void OnPbSessionStatusChanged(VOPlaybackSession* pPbSession);

pPbSession parameter: a pointer to the playback session object whose
5 status has changed.

void OnPbSessionStatusChanged is called when the playback session's
status has changed so that the UI can be updated accordingly.

10 **void OnConnStatusChanged(VOConnection* pConnection);**

pConnection parameter: a pointer to the connection object whose status
has changed.

void OnConnStatusChanged is called when a connection's status has
15 changed so that the UI can be updated accordingly.

void OnCallStatusChanged(VOCall* pCall);

pCall parameter: a pointer to the playback session object whose status has
changed.

20

void OnCallStatusChanged is called when the status of a call in the current
conference/playback session has changed so that the UI can be updated
accordingly.

25 **void OnPbCallStatusChanged(VOPbCall* pPbCall);**

pPbCall parameter: a pointer to the playback session object whose status
has changed.

void OnPbCallStatusChanged is called when the playback session's status
30 has changed so that the UI can be updated accordingly.

(VOConnection* pConnection);

-345-

pConnection parameter: a pointer to the Connection object whose status has changed.

void DisplayConnectionStatus is called to display a connection's status.

5

void DisplayCallStatus(VOCall* pCall);

pCall parameter: pointer to the call object whose status has changed.

void DisplayCallStatus is called to display a call's status (participant or
10 MCU).

void DisplayRecordingStatus(); is called to display the recording status if any call in a conference is being recorded.

15 **void DisplayWatchStatus();** is called to display the indication as to which call is being monitored, in the current conference or playback session.

void DisplayPlaybackStatus(); is called to display the playback status.

20 **Retcode OnDialSite();**

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

Retcode OnDialSite is called when the Dial button on the participant side is
25 clicked. This will dial the participant of selected connection.

Retcode OnDialMCU();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

30

Retcode OnDialMCU is called when the Dial button on the MCU side is clicked. This will dial the MCU port assigned to the selected participant.

-346-

Retcode OnHangupSite();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

5

Retcode OnHangupSite hangs up the call to the participant.

Retcode OnHangupMCU();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

10

Retcode OnHangupMCU hangs up the call to the MCU.

Retcode OnHoldSite();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

15

The Retcode OnHoldSite function puts the participant on hold (if the call is active).

20

Retcode OnHoldMCU();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

The Retcode OnHoldMCU function puts the MCU on hold (if the call is active).

25

Retcode OnWatchSite();

Return Value: returns a nonzero value if successful, zero otherwise.

30

The Retcode OnWatchSite function will monitor the current participant. The video stream corresponding to the participant will be displayed in the video

watch window.

Retcode OnWatchMCU();

Return Value: returns a nonzero value if successful, zero otherwise.

5

Retcode OnWatchMCU starts monitoring the MCU leg corresponding to a participant in a conference. The video stream is displayed in the video watch window.

10 **Retcode OnRecordMCU();**

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

Retcode OnRecordMCU starts recording the MCU stream. If the recording is already on, this function will pause/stop the recording.

15

Retcode OnRecordSite();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

20

Retcode OnRecordSite starts recording the stream corresponding the selected participant. If recording is already on, recording will pause/stop.

Retcode MakeAutoConnection();

25 Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

Retcode MakeAutoConnection is called to automatically connect the participant and the MCU and when successful, join them.

30

Retcode MakeAutoDisconnection();

Return Value: returns a nonzero value if the operation has been initiated

successfully, zero otherwise.

Retcode MakeAutoDisconnection is called to automatically un-join the connection and disconnect the calls to the participant and the mcu.

5

Retcode ConnectAll();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

10 Retcode ConnectAll is called to automatically make all the connection one by one.

Retcode DisconnectAll();

Return Value: returns a nonzero value if the operation has been initiated successfully, zero otherwise.

15

Retcode DisconnectAll is called to automatically break all the conference connections.

20

(f) *VOVideoWatchVw*

Class	VOMainFrame
Base Class	CFrameWnd
Inheritance Type	public
Friend Classes	-

(i) Attributes

Access Level	Type	Name	Description
protected	VOOperator*	m_pOperator	A pointer to the logged in video

-349-

			operator
	VOCallObjMgr*	m_pCallMgr	Pointer to the call object manager
	VOScheduleWnd*	m_pScheduleWnd	A pointer to the schedule window

(ii) Constructor(s)

VOVideoWatchVw();

5

(iii) Methods

void OnDial(); dials the number in the destination edit box.

10 **void OnTransfer();** transfers the current call to a number. This will initially display a dialog box where the user enters the number to which the call is to be transferred.

void OnAnswer(); is called when the Answer button is clicked.

15 **void OnForward();** is called when the forward button is clicked. All the call will be forwarded to the forwarding number provided.

void OnMute(); is called when the mute button is clicked. Turns the mute on/off.

20

void OnHangup(); is called when the hang-up button is clicked. Hangs up the current call.

25 **void OnHold();** is called when the hold button is clicked. Puts the current call on hold.

-350-

void OnPickup(); is called when the pickup button is clicked. Picks up the call on hold.

- 5 **void OnPrivacy();** is called when the privacy button is clicked. Turns the privacy on or off.

- 10 **void OnPlayMovie();** is called when the Play button is clicked. This will display a dialog box with a list of movies to choose from. Once a movie is selected, the movie will be played.

void OnRecordCall(); is called when the record button is clicked.

- 15 **void OnJoinToConference();** is called when the Join Conf button is clicked. This will display the list of active conferences and sites OR playback sessions. The operator will select the site corresponding to the current call and the call will be joined to the conference.

void WatchVideo(BOOL selection);

- 20 Return Value: returns a non-zero value if successful. zero otherwise
selection parameter: specifies what to watch.
selection = VDOWATCH_CONFERENCE displays the video from the site/MCU selected for watching
selection = VDOWATCH_SELF displays the output of the video operator's
25 camera
selection = VDOWATCH_CALL displays video from the call selected from the listbox provided in the video watch window OR the video from the incoming call, if any.

- 30 Call the void WatchVideo function to select the video stream to watch.

void OnDisplayCallsWindow(); is called when the 'Calls' button is clicked.

-351-

void OnSelfView(); is called when the 'SelfView' check box is checked or unchecked. When the self view is checked, the video operator's camera output is displayed in a separate small window.

5

void OnLocalVolume(); is called when the local volume slide bar position is changed. This will adjust the local volume.

10 **void OnRemoteVolume();** is called when the remote volume slide bar position is changed. This will adjust the remote volume signal.

b) Media Control Class Description

(1) VOMediaControl

Class	VOMediaControl
Base Class	VOObject
Inheritance Type	public
Friend Classes	-

15

(a) Attributes

Access Level	Type	Name	Description
protected	struct MtsLinkPortInfo	m_portInfo	This structure is used to communicate with the MCP

(b) Constructor(s)

VOMediaControl();

-352-

*(c) Methods***public void SetVolume(short rightVolume, short leftVolume);**

rightVolume parameter: an integer between 0 - 1000.

5 leftVolume parameter: an integer between 0 - 1000.

public void SetVolume sets the volume control.

public short GetVolume(short channel);

10 Return Value: returns the volume for the specified channel

channel parameter: set channel = PORT_CHANNEL_RIGHT for the right volume setting, and set channel = PORT_CHANNEL_LEFT for the left volume setting.

15 public short GetVolume returns the current volume for the specified channel

public void SetSelfView(long flags);

flags parameter: sets the properties of the self view. The valid flag values are:

20 SELFVIEW_ON Displays the self view;
SELFVIEW_OFF Hides the self view; and
SELFVIEW_MIRRORED Mirrors the self view.

public void SetSelfView sets the self view properties.

25

public long GetSelfView();

Return Value: returns the self view settings

The public long GetSelfView function returns the self view settings which
30 can be used to find out if the self view is visible or hidden, or if it is mirrored.

-353-

public void SetSelfViewSize(short size);

size parameter: one of the predefined sizes for the self view

- 5 public void SetSelfViewSize sets the size of the self view window. The valid values are FULL_CIF, HALF_CIF and QUARTER_CIF.

public short GetSelfViewSize();

Return Value: returns Current self view size.

10

The **public short GetSelfViewSize** function returns the current self view window size. The values will be one of the predefined sized. See SetSelfViewSize for the description of the sizes.

- 15 **public void SetAutoGain(BOOL autoGain = TRUE);**

autoGain parameter: should be TRUE to enable auto gain, FALSE to disable

The public void SetAutoGain function enables or disables the auto gain depending on the autoGain value.

20

public BOOL GetAutoGain();

Return Value: returns The current auto gain setting.

The public BOOL GetAutoGain function returns the current auto gain setting. TRUE if auto gain is on, FALSE otherwise.

25

public void SetEchoCancellation (bool bCancel);

bCancel parameter: if bCancel is TRUE cancellation is enabled; if FALSE cancellation is disabled.

30

public void SetEchoCancellation enables or disables echo cancellation.

-354-

public BOOL GetEchoCancellation ();

Return Value: returns the current echo cancellation state.

public BOOL GetEchoCancellation gets the current state of the current
5 echo cancellation.

public short GetVideoMode(short mode = MODE_RX);

Return Value: returns the video mode

mode parameter: indicates receive or transmit mode.

10

public short GetVideoMode gets the audio mode for receive or transmit,
depending on the value of mode. mode = MODE_RX for receive mode and
MODE_TX for transmit.

15 **public short GetAudioMode(short mode = MODE_RX);**

Return Value: returns the audio mode

mode parameter: indicates receive or transmit mode.

public short GetAudioMode gets the audio mode for receive or transmit,
20 depending on the value of mode. mode = MODE_RX for receive mode and
MODE_TX for transmit.

public void SetVideoWnd(HWND hWnd);

hWnd parameter: pointer to the window where the video is to be displayed.

25

The public void SetVideoWnd function displays the video in the window
identified by hWnd.

public HWND GetVideoWnd();

30 Return Value: returns the window handle in which the video is being
displayed. If no window is set, NULL is returned.

-355-

The public HWND GetVideoWnd function is called to retrieve the window handle in which the video is being displayed.

public void MakeVideoWndResizable(BOOL bResize = TRUE);

- 5 bResize parameter: if bResize is TRUE, the video window is resizable; if FALSE, it is not resizable.

The public void MakeVideoWndResizable function makes the video window resizable with bResize = TRUE. To make the window fixed size, make bResize

- 10 FALSE.

public BOOL IsVideoWndResizable();

Return Value: returns TRUE if the video window is resizable, FALSE otherwise.

15

Call the public BOOL IsVideoWndResizable function to determine if the video window is resizable.

F. Video Operator Shared Database

- 20 1. Database Schema

Figure **107** shows a database schema for the video operator shared database (see **40214** Figure **98**). In one embodiment, the database contains the following tables. CONFERENCE **41104** lists details about a scheduled conference, PARTICIPANT **41105** lists the participants of conferences, and

25 CONF_PARTICIPANT **41108** contains the keys from the CONFERENCE **41104** and PARTICIPANT **41105** tables, which are used to determine the participants in any given conference. MCU **41102** contains the characteristics of different MCU's from various suppliers, and MCUPORT **41106** contains the MCU identification number from the MCU **41102** table

30 as well as the ports of the MCU used by the participants to connect to a

conference. VOPERATOR lists video operator attributes; VOTYPES lists all the types (e.g., protocols, bandwidths) used to define a conference or participant; and VOTYPEVALUES **41107** lists the values for each of the defined types.

5

Each video operator record in the VDO_OPERATOR **41101** table contains a unique identification number in its ID field, which number may appear in the CONFERENCE **41104** table's operatorID field, assigning each video operator to particular conferences profiled in the CONFERENCE **41104** table. Each conference record in the CONFERENCE **41104** table, in turn, contains a unique identification number in its ID field, which number may appear in the CONF_PARTICIPANT **41108** table's confID field. Similarly, each participant record in the PARTICIPANT **41105** table contains a unique identification number in its ID field, which number may appear in the CONF_PARTICIPANT **41108** table's participantID field. Finally, each MCU record in the MCU **41102** table contains a unique identification number in its ID field, which number may appear in the MCUPORT **41106** table's mcuID field, identifying the set of MCU ports associated with the MCU. Each MCU port record in the MCUPORT **41106** table, in turn, contains a unique identification number in its ID field, which number may appear in the CONF_PARTICIPANT **41108** table's mcuPortID field. Within the CONF_PARTICIPANT **41108** table, the confID, participantID, and mcuPortID values are used as cross-referencing keys to define a particular conference with a given conference profile, a set of participants, and an MCU port.

25

In addition, each VOType record in the VOTYPE **41103** table contains a unique identification number in its ID field, which number may appear in the VOTYPEVALUES **41107** table's typeID field, identifying a set of values associated with the VOType.

30

G. Video Operator Console Graphical User Interface Windows

1. Main Console Window

Figure **108** shows one embodiment of the Main Console window **41201** as it would appear on a Video Operator Terminal [**1** Figure **96**], showing possible
5 placements of a Schedule window **41202**, a Conference window **41203**, a Video Watch window **41204** and a Console Output window **41205**. The Main Console window **41201** enables the video operator to manage video conferences.

2. Schedule Window

Figure **109** shows one embodiment of the Schedule window **41202**, which displays all the conferences **41305** and playback sessions **41306** to be
10 handled by the current video operator for the next 8 hours. In one embodiment, the list is updated upon application startup, at 15 minute intervals, and every time a conference ends.

The Schedule window will have two scrolled text areas - one area for conferences **41301**, and the other for sites **41302** participating in the
selected conference. If a conference name is double-clicked, the appropriate
20 Conference Window [**41203** Figures **108**, **110**] will appear.

3. Conference Window

Figure **110** shows one embodiment of the Conference window **41203**, which is displayed when the operator selects a conference or playback session in
25 the Schedule window **41202**. The display of the Conference Window **41203** is dependent on whether a Conference or a Playback Session has been selected from the Schedule Window **41202**. Only one conference window is displayed at a time. When a new conference window is opened, the existing one is hidden. While a Conference Window is hidden, the status of the

-358-

conference and connections are still monitored. Figure **110** shows a Conference Session **41401**. The Conference window **41203** displays the list of conference Participants **41415** and radio buttons to selectively operate on individual connections, including call setup, viewing, playback and
5 recording.

Information about the conference such as the duration, start time, end time, playback and recording status, and conference type are displayed at the bottom of the window. If the operator double clicks inside the Conference
10 Window **41203** where there is no action associated with the clicking location, the Properties Box [**41701** Figure **113**] is displayed with the conference settings.

A conference is ended by pressing the End Conference button. This will
15 disconnect all calls associated with the conference.

The Conference Window **41203** displays the connections in the conference and their connection status **41417**, including any free MCU Port slots reserved for a not yet joined connection **41421**. Each Connection listing
20 contains a radio button **41422**, the participant site name **41423** and status lights **41418-41420**. The status of the two calls and the join are monitored and displayed with the site name in the Conference window **41203**. The status squares **41418-41420** are colored boxes, with different colors representing different call statuses (e.g., no call, call in progress, active call,
25 or active call that has been disconnected).

The Conference Window **41203** provides buttons to click **41417** that define the sequence in which a participant site gets connected to an MCU Port site, routed through the video operator. Other features available from this part of
30 the window are watching the video input from a call, recording video input from either call, and making a normal video call to the participant site or to the MCU.

-359-

The color of the arrows **41424** represents the status of each call. The color of the arrows is also duplicated in the status lights **41418-41420** in the list of connections.

5

If there is a Playback Connection **41425** associated with the Conference, only one Call is necessary to an MCU Port site. The normal Participant Site call setup interface will be inaccessible, and the Join control **41405** will become the Start and Stop switch for playback.

10

Free MCU ports can be reached only when an MCU Port call for a defined Connection is inactive (or disconnected). This allows the operator to join a conference as if the operator were a participant. This is done by selecting the Connection with the free MCU port call. When connected, the operator can inform the rest of the participants that the operator is attempting to contact or restore a connection.

15

There are some functional limitations that the Conference Window **41203** will reflect. The Conference Window **41203** should not allow access to functions that cannot be performed, for example:

20

- The video operator can only view one call at a time.
- The video operator can record any call at any time with software unidirectional decoder.
- 25 • Playback connection selection changes the call setup buttons appropriately.
- The video operator can participate in a conference only when a MCU port call is inactive.
- The video operator can talk to participant site only when the participant is disconnected.

30

-360-

To clarify, a simple connection setup using the Conference Window proceeds as follows. By pressing the Call button near the participant site box **41402**, the operator calls Adam (or, alternatively, Adam may call the operator), and then the operator places the call on Hold **41407**. By pressing the Call
5 button near the MCU Port site box **41403**, the operator calls the MCU and then places the call on Hold **41408**. By pressing the Join button **41405**, the two calls are joined. In another embodiment, this can be an automated rather than a manual process. Adam and the MCU are now connected as H.320 video call. All three arrows **41424** will be green.

10

4. Video Watch Window

Figure **111** shows one embodiment of the Video Watch window **41204**, which displays the H.320 input from a selected call of a conference connection or a separate incoming or outgoing call. The Video Watch
15 window **41204** also has controls for making normal calls **41512** and media control such as audio control **41509-41510**.

The Video Watch window is the display for the unidirectional H.320 decode of the video output of a selected call. By default, the MCU call of the first
20 active site will be displayed. To watch any other call, the appropriate View button must be pressed in the Conference Windows. The video and audio controls for this window such as volume control **41509-41510**, picture size **41511**, etc., are managed from the Video Control Panel.

25 When the operator chooses to make a normal H.320 video call (point to point), to a site or an available slot in an active conference, the Video Watch window **41204** is used for viewing the video. A small self-view video window should appear nearby when the operator selects the Self View button **41506**.

30

-361-

5. Console Output Window

Figure **112** shows one embodiment of the Console Output window **41205** which displays all error messages and alerts **41601**. The window is scrollable so that the video operator can see all errors that have occurred in the current session. These messages are also logged to a text file for future reference.

6. Properties Dialog Box

Figure **113** shows a Properties dialog box **41701**. Dialog boxes are windows that are transitional and only displayed temporarily. They are usually used for entering data or displaying information that requires immediate attention. This will be a modeless dialog box displaying the properties of a particular conference or site. There will be only one such window open at any time. If the user focuses on another Conference Window or Connection Window, the same dialog box is updated with the appropriate properties. Figure **113** pictures the properties associated with a particular site, including the site coordinator **41702**, the site phone number **41703**, the time **41704**, connection type **41705** and terminal type **41706**. A Close button **41707** closes the Properties dialog box **41701**.

XVII. WORLD WIDE WEB (WWW) BROWSER CAPABILITIES

A. User Interface

The graphical user interface is designed such that only a single IP connection from the workstation to the server is required. This single IP connection supports both the Internet connection between the WWW Browser and the WWW Site, and the messaging connection between the PC Client and the universal inbox (i.e., Message Center). The PC Client interface is integrated with the WWW Browser interface such that both components can exist on the same workstation and share a single IP connection without

-362-

causing conflicts between the two applications.

WWW Browser access is supported from any of the commercially available WWW Browser interfaces:

- 5 • Microsoft Internet Explorer;
- Netscape Navigator (1.2, 2.X); or
- Spyglass Mosaic.

In addition, the WWW Browser interface is optimized to support Windows 95; however, Windows 3.1 and Windows 3.11 are supported as well.

10

The WWW Browser interface detects the display characteristics of the user's workstation (or terminal) and adapts the presentation to support the display settings of the workstation. The presentation optimized around a 640x480 pixel display but is also capable of taking advantage of enhanced resolution and display qualities of 800x600 (and greater) monitors.

15

To improve performance, the user is able to select between 'minimal graphics' or 'full graphics' presentation. The WWW browser will detect whether a user has selected 'minimal graphics' or 'full graphics' and send only the appropriate graphics files.

20

B. Performance

Response time for downloading of information from the WWW Site or the Personal Home Page to the user's workstation or terminal meets the following benchmarks.

25

Workstation Configuration:

- Processor: 486DX - 33 MHz;
- Memory: 12 MB;
- Monitor: VGA, Super VGA, or XGA;
- 30 • Access: Dialup;
- Windows 95;

-363-

- Presentation Option: Full Graphics; and
- Peripherals: Audio Card, Audio Player Software, 14.4 Kbps Modem.

REQUIREMENT	MEAN VALUE	NOT TO EXCEED VALUE
Retrieve and Personal Home Pages. Time is measured from when the user selects the Bookmark until the Status Bar reads, "Document: Done".	20 sec	30 sec
Retrieve WWW screens other than Home Pages. Time is measured from when the user selects the hypertext link or tab until the Status Bar reads, "Document: Done".	5 sec (text only) or 15 sec (scheduling screen)	15 sec (text only) or 30 sec (scheduling screen)

Start playing a voicemail message. Time is measured from when the users selects the voicemail message in the Message Center until the streaming audio file starts playing on the user's workstation.	10 sec	15 sec
--	--------	--------

5

After a screen or page has been downloaded from the WWW Site to the workstation, the cursor is pre-positioned onto the first required field or field that can be updated.

C. *Personal Home Page*

The system provides subscribers the ability to establish a Personal Home Page which provides a vehicle for people to communicate with or schedule meetings with the subscriber. A person accessing a subscriber's Personal Home Page is referred to as the guest and the user that 'owns' the Personal Home Page is referred to as the subscriber.

Guest-access to Personal Home Pages will support the following features:

- Create and send a text-based pager message through networkMCI Paging;
- Create and send an email message to the email (MCI Mail or internetMCI) account; and
- Access the subscriber's calendar to schedule a meeting.

Messages generated through the subscriber's Personal Home Page are directed to the subscriber's networkMCI or SkyTel Pager, or MCI email account.

Email messages composed by guests will:

- Present the subscriber's name, not the subscriber's email address, in the email header;
- Provide a field in the email header for the:
 - Sender's name (required field),
 - Sender's email address (optional field), and
 - Subject (optional field).

Guests 'request' appointments on a subscriber's Personal Home Page.

- Requested appointments on a subscriber's Personal Home Page will be prefaced with "(R)".
- Approved appointments will be prefaced with "(A)".

-365-

Subscribers are responsible for routinely checking their calendars and approving "(A)" or deleting requested appointments, and initiating the necessary follow-up communications to the requesting party. Approved
5 appointments will be prefaced by "(A)".

Security Requirements

Calendar access from the Personal Home Page is designed to support two-levels of security:

- No PIN Access:

- 10 -Times Only, or
- Times & Events;

- PIN Access:

- Times Only; or
- Times & Events.

15

1. Storage Requirements

The system stores and maintains past and future appointments in the following manner:

- Current month plus past six months of historical calendar appointments
- 20 • Current month plus next twelve months of future calendar appointments.

A subscriber is provided the option to download the contents of the months appointments that are scheduled to be overwritten in the database. The calendar information that will be downloaded to the subscriber is in a comma delimited or DBF format and capable of being imported into
25 Microsoft Schedule+, ACT or Ascend.

-366-

2. On Screen Help Text

On screen help text provides guest and subscriber icon access to field specific "Help" instructions to operate within the Personal Home Page. The Help Text must provide information describing:

- 5 • How to Send the subscriber a text-based pager message from the Personal Home Page through networkMCI Paging;
- How to Send the subscriber an email message from the Personal Home Page to an MCI email account;
- How to Access and update a subscriber's Calendar;
- 10 • How to Locate a user's Personal Home Page; and
- How to Order your own Personal Home Page through MCI.

3. Personal Home Page Directory

- The provides the guest the ability to access to a Personal Home Page
- 15 directory through the existing MCI Home Page. This directory allows the guest to search all established Personal Home Page accounts for a specific Personal Home Page address, by specifying Last Name (required); First Name (optional), Organization (optional), State (optional) and/or Zip Code (optional). Results from the Personal Home Page directory search return the
- 20 following information: Last Name, First Name, Middle Initial, Organization, City, State and Zip Code. Although City is not requested in search criteria it is provided in search results.

- Another means for a guest to locate a Personal Home Page is through the
- 25 WWW Browser. Many WWW Browsers have built in search capabilities for 'Net Directory.' Users' Personal Home Pages are listed within the directories of Internet addresses presented by the WWW Browser. The benefit to conducting your search from the MCI Home Page is that only Personal Home

-367-

Pages are indexed (and searched). Conducting the search through the WWW Browser menu option will not limit the search to Personal Home Pages and therefore will conduct a search through a larger list of URLs. In addition, guests have the capability to enter the specific URL (i.e., Open Location) for the Personal Home Page rather than performing a search. This is especially important for those subscribers that have their Personal Home Page “unlisted” in the directory.

4. Control Bar

10 A Control Bar is presented at the bottom of the Personal Home Page. The Control Bar is presented after the guest has selected Personal Home Pages from the MCI Home Page. The Control Bar provides the guest access to the following features:

- Help Text
- 15 • MCI Home Page
- Personal Home Page Directory
- Feedback.

5. Home Page

20 The Home Page is the point of entry for the subscriber to perform message retrieval and exercise profile management from a WWW Browser. The Home Page is designed to provide the user easy access to the Message Center or Profile Management.

25 6. Security Requirements

Access to the Message Center or Profile Management is limited to authorized

-368-

- users. Users are prompted to enter their User ID and Password before accessing the Message Center or Profile Management. After three unsuccessful attempts, the user is blocked from accessing the Message Center or Profile Management and a WARNING message advises the subscriber to contact the MCI Customer Support Group. The account is deactivated until an MCI Customer Support representative restores the account. After the account is restored, the subscriber is required to update his or her Password.
- 10 A successful logon to the Message Center enables the user to access Profile Management without being challenged for another (i.e., the same) User ID and Password. The same is also true for users that successfully access Profile Management — they are allowed to access the Message Center without being challenged for another (i.e., the same) User ID and Password.
- 15 Passwords are valid for one month. Users are prompted to update their password if it has expired. Updates to passwords require the user to enter the expired password, and the new password twice.

7. On Screen Help Text

- 20 Provide the subscriber icon access to field specific “Help” instructions to operate within the Home Page. The Help Text provides information describing:
- How to Access Message Center;
 - How to Access Profile Management;
 - 25 • How to Access the MCI Home Page;
 - How to Access Personal Home Pages;
 - How to Send (i.e. Create or Forward) Messages through Message Center;
 - How to File Messages through Message Center;

-369-

- How to Update the directlineMCI Profile;
 - How to Update the Information Services Profile;
 - How to Update their Personal Home Page;
 - How to Provide Feedback on the Home Page; and
- 5 • How to Order the User's Guide.

Control Bar

A Control Bar is presented at the bottom of the Home Page. The Control Bar provides the guest access to the following features:

- Help Text;
- 10 • MCI Home Page;
- Personal Home Page Directory; and
 - Feedback.

8. Profile Management

- In addition to the On-Screen Help Text and Control Bar discussed above, the
- 15 Profile Management screen presents a Title Bar. The Title Bar provides the subscriber easy access to the Profile Management components and quick access to the Message Center. Access to the Profile Management components is provided through the use of tabs which will include:

- directlineMCI;
- 20 • Information Services;
- Personal Home Page;
 - List Management; and
 - Message Handling.

- The directlineMCI tab includes additional tabs for the underlying
- 25 components of directlineMCI which are:

- Voicemail;

-370-

- FAXmail;
- Paging.

The directlineMCI Profile Management system provides subscribers a Profile Management page from which account profile information can be

5 manipulated to:

- Create new directlineMCI profiles and assign names to the profile;
- Update existing directlineMCI profiles;
- Support the rules-based logic of creating and updating directlineMCI profiles (e.g., selection of only one call routing option, like voicemail, invokes
10 override routing to voicemail; and updates made in one screen ripple through all affected screens, like paging notification);
- Enable a directlineMCI number;
- Enable and define override routing number;
- Enable and define FollowMe routing; and
- 15 • Define RNA parameters for each number in the directlineMCI FollowMe routing sequence
- Enable and define final routing (formerly called alternate routing) to:
 - Voicemail and pager,
 - Voicemail only,
 - 20 -Pager only, and
 - Final message;
 - Invoke menu routing if two or more of the call routing options (FollowMe, voicemail, faxmail or pager) are enabled;
 - Enable voicemail;
 - 25 • Enable faxmail;
 - Enable paging;

-371-

- Define the default number for faxmail delivery;
 - Activate paging notification for voicemail;
 - Activate paging notification for faxmail;
 - Define schedules to activate/deactivate different directlineMCI profiles;
- 5 • Provide guest option to classify voicemails for urgent delivery;
- Configure the time zone for all message types that will be used to identify the time a message is received;
 - Define call screening parameters for:
 - Name and ANI,
- 10 -ANI only, and
- Name only; and
 - Enable or disabling park and page.

9. Information Services Profile Management

- 15 Information Services Profile Management provides subscribers the ability to select the information source, delivery mechanism (voicemail, pager, email) and the delivery frequency depending upon the information source and content. Specifically, the subscriber has the ability configure any of the following information sources:
- 20 • Stock Quotes and Financial News; and
- Headline News.
- Stock Quotes and Financial News provides the subscriber the following:
- Business News Headlines;
 - Stock Quotes (delay less than or equal to 10 minutes);
- 25 • Stock Market Reports (hourly, AM/PM or COB);

-372-

- Currency and Bond Reports (hourly, AM/PM or COB);
- Precious Metal Reports (hourly, AM/PM or COB); and
- Commodities Reports (hourly, AM/PM or COB).

5 Business News Headlines are delivered via email once per day. Reports
(Stock Market, Currency and Bond, Precious Metal and Commodities) are
delivered at the interval specified by the subscriber. Hourly reports require
that email message is time stamped at 10 minutes after the hour. AM/PM
reports require that one email message is transmitted in the morning (11:10
10 am ET) and one email message is transmitted in the evening (5:10 PM ET),
with COB reports transmitted at 5:10 PM ET.

The content of the Stock Market Report contains:

- Stock or mutual fund ticker symbol;
- 15 • Stock or mutual fund opening price;
- Stock or mutual fund closing price;
- Last recorded bid price for the stock or mutual fund;
- Last recorded ask price for the stock or mutual fund;
- Stock or mutual fund's 52-week high; and
- 20 • Stock or mutual fund 52-week low.

Stock Quotes and Financial News also provide the subscriber the ability to
select from a list of available stocks and mutual funds and define criteria
whereby a voicemail or text-based page is provided. The definable criteria
25 are referred to as 'trigger points' and can be any or all of the following
conditions:

- Stock or mutual fund reaches a 52-week high value;

-373-

- Stock or mutual fund reaches a 52-week low value;
- Stock or mutual fund reaches a user-defined high point; and
- Stock or mutual fund reaches a user-defined low-point.

5 After a 'trigger point' condition has been satisfied, a message (voicemail or text-based pager) is transmitted within 1 minute to the subscriber. Voicemail messages are directed to the subscriber's mailbox defined in the user's directlineMCI account. The information content for Stock Quotes and Financial News is no older-than 10-minutes old.

10

10. Personal Home Page Profile Management

Personal Home Page Profile Management provides subscribers the ability to customize their Personal Home Page and define how guests can communicate with them (email or text-based pager). In addition, Profile Management also enables subscribers to control guest access to their calendar. Specifically, the subscriber is able to:

15

- Establish and maintain a greeting message;
- Establish and maintain a contact information (i.e., address information);
- Establish and maintain a personal calendar;
- 20 • Enable or disable guest access to paging, email or calendar;
- Control guest access to calendar by defining PINs for standard or privileged access; and
- Incorporate an approved subscriber submitted graphic, such as a personal photo or corporate logo, on a predefined location on the Personal Home
- 25 Page.

Upon creation of the Personal Home Page, the contact information is

-374-

populated with the subscriber's delivery address information. The subscriber has the capability to update that address information contained within the contact information.

11. List Management

5 **List Management** provides the subscriber the ability to create and update lists. Profile Management provides subscribers the ability to define lists accessible through the Message Center for message distribution. In one embodiment, list management is centralized such that Fax Broadcast list management capabilities are integrated with directlineMCI list management
10 capabilities to provide a single database of lists. In an alternate embodiment, the two list management systems are separate, so the user may access either database for lists.

15 Lists are maintained through an interface similar to an address book on the PC Client whereby subscriber are able to add or remove names to lists. Associated with each person's name are the email address, faxmail address (i.e., ANI), voicemail address (i.e., ANI), and pager number. As messages populate the Message Center inbox (i.e., universal inbox), the address book is updated with the source address of the associated message type.

20

When a subscriber chooses to create a distribution list, she is prompted to select a name, type and identifier name for the list. All created lists are available in alphabetical order by name. The type of the list (voice, fax, email, page) accompanies the list name. In addition, list identifiers may
25 consist of alphabetic characters.

The subscriber is then prompted for recipient names and addresses to create a distribution list. The subscriber is able to access his address book for recipient information. The subscriber is not be restricted to record the

-375-

same address types in his list; if a list is created with a fax type, the subscriber is able to include ANI, email and paging addresses in the list. The subscriber is able to manage his distribution lists with create, review, delete, edit (add and delete recipients) and rename capabilities.

5

When the user chooses to modify a list through the WWW Browser interface, she is prompted to select the address type (voice, fax, fax, paging, email) and a list of the user's distribution lists should be provided for that address type. The user is also able to enter the List Name to locate it. Users are able
10 to modify lists through create, review, edit (add and remove recipients), delete and rename commands.

Whenever a subscriber modifies a list with a recipient addition, removal or address change, she is able to make the modification a global change. For
15 example, a user changes the voice mailbox address for Mr. Brown in one list. she is able to make this a global change, changing that address for Mr. Brown in all of his distribution lists. While the subscriber is able to create and modify distribution lists through the ARU and VRU in addition to the PC, enhanced list maintenance capabilities are supported through the WWW
20 Browser interface.

The subscriber is able to search and sort lists by name or by the different address fields. For example, a user is able to search for all lists containing 'DOLE' by using the *DOLE* command within the search function. In
25 addition, users are able to search lists using any of the address fields. For example, a user could search based on a recipient number, 'to' name or zip code. A user is able to sort lists by list names, identifiers and types or by any address field.

-376-

In addition to search capabilities, the distribution list software enables the user to copy and create sub-lists from existing distribution list records. The user is able to import and export recipient data from external database structures.

5

The capability to share lists among users and upload lists to a host also exists.

12. Global Message Handling

10 Global Message Handling provides subscribers the ability to define the message types that will appear in the "universal inbox" or accessed through the Message Center. The following message types are selectable:

- directlineMCI voicemail;
- directlineMCI faxmail;
- 15 • networkMCI and SkyTel Paging; and
- Email from an MCI email account (i.e., MCI Mail or internetMCI).

If a subscriber is not enrolled in a specific service then that option will be grayed-out and therefore not selectable within Global Message Handling.

20 Any updates to Global Message Handling result in a real-time update to the Message Center. An example is that a subscriber may choose to allow voicemail messages to appear in the Message Center. The Message Center automatically retrieves all voicemail message objects that exist within the voicemail database.

25 **D. Message Center**

The Message Center functions as the "universal inbox" for retrieving and manipulating message objects. The "universal inbox" consists of folders

-377-

containing messages addressed to the user. Access to the Message Center is supported from all WWW Browsers, but content contained in the "universal inbox" only presents the following message types:

- Voicemail: addressed to user's directlineMCI account;
- 5 • Email: addressed to the user's MCI email (i.e., MCI Mail or internetMCI) account;
- FAXmail: addressed to the user's directlineMCI account; and
- Paging: addressed to the user's networkMCI Paging account (or SkyTel Paging account).

10

In addition to the On-Screen Help Text and Control Bar discussed in the previous sections, the Message Center screen presents a Title Bar. The Title Bar provides the subscriber easy access to the Message Center functions and quick access to Profile Management. The Message Center functions that
15 are supported through the Title Bar are:

- File: lists user's defined folders and allows user to select folder;
- Create: compose a new email message;
- Forward: voicemails will be forwarded as email attachments;
- Search: provide ability to search based on message type, sender's name or
20 address, subject or date/time; and
- Save: allows users to save messages to a folder on the universal inbox, to a file on the workstation or to a diskette.

When composing or forwarding messages through the Message Center, the
25 user has the ability to send a message as either an email or a faxmail. The only limitation is that voicemails may only be forwarded as voicemails or as email attachments. All other message types may be interchanged such that emails may be forwarded to a fax machine, or pager messages may be

-378-

forwarded as an email text message. Messages that are sent out as faxmail messages are generated in a G3 format, and support distribution to Fax Broadcast lists.

- 5 The presentation layout of the Message Center is consistent with the presentation layout of the PC Client such that they have the same look and feel. The Message Center is designed to present a Message Header Frame and a Message Preview Frame, similar to the presentation that is supported by nMB v3.x. The user will have the ability to dynamically re-size the height
- 10 of the Message Header Frame and the Message Preview Frame. The Message Header Frame will display the following envelope information:
- Message type (email, voice, fax, page);
 - Sender's name, ANI or email address;
 - Subject;
 - 15 • Date/time; and
 - Message size.

The Message Preview Frame displays the initial lines of the body of the email message, the initial lines of the first page of the faxmail message, the pager

20 message, or instructions on how to play the voicemail message. Playing of voicemail messages through an WWW Browser is supported as a streaming audio capability such that the subscriber is not required to download the audio file to their workstation before playing it. The streaming audio is initiated after the user has selected (single left-mouse click) on the voicemail

25 header in the Message Header Frame. Displaying of faxmail messages is initiated immediately after the user has selected (single left-mouse click) on the faxmail header in the Message Header Frame.

-379-

The Message Center also allows the subscriber to use distribution lists that have been created in Profile Management. The distribution lists support sending messages across different message types.

In addition to the basic message retrieval and message distribution, the Message Center supports the creation and maintenance of message folders (or directories) within the universal inbox. Initially users are limited to the following folders:

- Draft: retains all saved messages that have NOT been sent;
- Inbox: retains all messages received by the “universal inbox” and it will be the default folder presented when the user accesses Message Center;
- Sent: retains all messages that have been sent; and
- Trash: retains for 7 days all messages marked for delete. Subscribers will eventually be able to create (and rename) folders (and folders within folders).

1. Storage Requirements

Initially, users are allotted a limited amount of storage space for directlineMCI voicemail and directlineMCI faxmail. Pager recall messages and email messages are not limited based upon amount of storage space consumed, but rather the date/time stamp of the message received.

Ultimately, storage requirements will be enforced based upon a common measurement unit, like days. This will provide users an easier approach to knowing when messages will be deleted from the database, and when guests will be prevented from depositing a message (voicemail, faxmail) to their “universal inbox”. To support this, the following are storage requirements for messages retained in the inbox:

- directlineMCI voicemail: 60 minutes;
- directlineMCI faxmail: 50 pages;
- networkMCI pages: 99 hours; and

-380-

- Email: 6 months.

The subscriber is provided the option to download the messages that are scheduled to be overwritten in the database except for messages that are
5 retained in the trash folder.

E. PC Client Capabilities

1. User Interface

- 10 The PC Client interface supports subscribers that want to operate in a store & forward environment. These users want to download messages to either manipulate or store locally. The PC Client is not designed to support Profile Management and the PC Client interface only presents messages (voicemail, faxmail, email, text-page). Access to Profile Management capabilities only is
15 available through the ARU interface or the WWW Browser interface. The PC Client interface is integrated with the WWW Browser interface such that both components can exist on the same workstation and share a single IP connection.
- 20 The PC Client interface is optimized to support Windows 95; however, Windows 3.1 is supported as well.

The graphical user interface is designed to present a Message Header Window and a Message Preview Window, similar to the presentation that is
25 supported by nMB v3.x and is supported by the WWW Browser. The user has the ability to dynamically re-size the height of the Message Header Window and the Message Preview Window. The Message Header Window

-381-

displays the following envelope information:

- Message type (email, voice, fax, page);
- Sender's name, ANI or email address;
- Subject;
- 5 • Date/time; and
- Message size.

The Message Preview Window displays the initial lines of the body of email messages or pager messages, or instructions on how to display the faxmail message or play the voicemail message. Playing of voicemail messages from
10 the PC Client requires an audio card be present on the PC. Displaying of faxmail messages invokes the faxmail reader within the PC Client.

The Message Center also allows the user to use distribution lists that have been created in Profile Management. The distribution lists support sending
15 messages across different message types.

2. Security

User authentication between the PC Client and the server is negotiated during the dial-up logon session. Security is supported such that the User
20 ID and Password information is imbedded in the information that is passed between the PC Client and server when establishing the interface. Subscribers are not required to manually enter their User ID and Password. In addition, updates made to the password are communicated to the PC Client.

25

3. Message Retrieval

Message Retrieval provides subscribers the ability to selectively retrieve

-382-

voicemail, faxmail, pages and email messages that reside in the "universal inbox". Message types that are displayed or played from the PC Client include:

- directlineMCI voicemail;
- 5 • directlineMCI faxmail;
- networkMCI paging; and
- Email from an MCI email account;

The PC Client initiates a single communication session to retrieve all message types from the "universal inbox". This single communication session is able to access the upstream databases containing voicemails, 10 faxmails, emails and pages.

The PC Client also is able to perform selective message retrieval such that the user may is able to:

- 15 • Retrieve all messages;
- Retrieve full text (or body) for selected message header(s);
- Retrieve messages based upon editable search criteria:
 - priority messages;
 - email messages;
 - 20 -pager messages;
 - faxmail messages (complete or header only);
 - voicemail messages (complete or header only);
 - sender name, address or ANI;
 - date/time stamp on message; and
 - 25 -message size.

-383-

Header-only faxmail messages retrieved from the "universal inbox" are retained in the "universal inbox" until the message body is retrieved.

Voicemail messages are retained in the "universal inbox" until the subscriber accesses the "universal inbox" via the WWW Browser (i.e.,

5 Message Center) or ARU and deletes the message. Messages retrieved from the "universal inbox" are moved to the desktop folder.

In addition, the PC Client is able to support background and scheduled polling such that users are able to perform message manipulation (create,

10 edit, delete, forward, save, etc.) while the PC Client is retrieving messages.

4. Message Manipulation

Message Manipulation provides subscribers the ability to perform many standard messaging client actions, like:

- 15 • Compose (or create) email, faxmail or pager messages;
- Forward all message types;
- Save;
- Edit;
- Delete;
- 20 • Distribute;
- Attach;
- Search; and
- Display or play messages.

F. Order Entry Requirements

25 directlineMCI or networkMCI Business customers are provided additional interface options to perform profile management and message management

-384-

functions. Both directlineMCI and networkMCI Business customers are automatically provided accounts to access the features and functions available through the different interface types. The ability to provide accounts to networkMCI Business customers is also supported; however not all networkMCI Business customers are provided accounts. Order entry is flexible enough to generate accounts for networkMCI Business customers, as needed.

Order entry is designed such that directlineMCI customers or networkMCI Business customers are automatically provided access to the additional interface types and services provided in the system. For example, a customer that orders directlineMCI (or networkMCI Business) is provided an account to access the Home Page for Profile Management or Message Center. Checks are in place to prevent a customer from being configured with two accounts — one from directlineMCI and one from networkMCI Business. In order to accomplish this, integration between the two order entry procedures is established.

An integrated approach to order entry requires a single interface. The interface integrates order entry capabilities such that the order entry appears to be housed in one order entry system and does not require the order entry administrator to establish independent logon sessions to multiple order entry systems. This integrated order entry interface supports a consistent order entry methodology for all of the services and is capable of pulling information from the necessary order entry systems. In addition, the interface supports the capability to see the services associated with the user's existing application.

The specific requirements of the integrated order interface system are:

- Automated feeds to define an MCI email (MCI Mail or internetMCI) account;

-385-

- Automated feeds to define a networkMCI paging account(or SkyTel Paging) account;
 - Automated feeds to define a directlineMCI account;
 - Automated feeds to enable Fax Broadcast capabilities;
- 5 • Ability to manually enter MCI email account, networkMCI paging account or directlineMCI account information;
- Ability to enable or disable access to inbound information services; and
 - Ability to enable or disable access to outbound information services.
- 10 These abilities give order entry administrators the flexibility to add a user based upon preexisting MCI service (email, paging, directlineMCI) account information. Alternatively, the order administrator may add a user while specifying the underlying services.
- 15 The order entry systems provide the necessary customer account and service information to the downstream billing systems. They also track the initial customer order and all subsequent updates so that MCI can avoid sending duplicate platform software (i.e., PC Client) and documentation (i.e., User Guide). In addition, order entry processes enable an administrator to
- 20 obtain the following information:
- Record customer delivery and name:
 - support USA and Canadian addresses, and
 - provide ability to prevent delivery to P.O. boxes;
 - Record customer's billing address, phone number and contact name;
- 25 • Record the order date and all subsequent updates;
- Record the name, phone number and division of the Account Representative that submitted the order;

-386-

- Record or obtain the user's directlineMCI number;
- Record or obtain the user's networkMCI paging PIN;
- Record or obtain the user's MCI email account ID;
- Generate a daily Fulfillment Report that is electronically sent to fulfillment
5 house; and
- Generate a daily Report that tracks:
 - number of orders received;
 - number of orders to create networkMCI Paging (or SkyTel Paging) account;
 - number of orders to create MCI email account, and
 - 10 -number of orders to create a directlineMCI account.

Personal home pages can be ordered for a customer. The customer delivery
information recorded during order entry is the default address information
that is presented from the user's Personal Home Page. In addition, the order
15 entry processes support the installation of and charging for special graphics.

The capability to turn existing feature/functionality 'on' and 'off' for a
specific service exists. Features that can be managed by the user are
identified within the order entry systems. These features are then activated
20 for management within the user's directory account.

There are real-time access capabilities between order entry systems and the
user's directory account. This account houses all of the user's services,
product feature/functionality, and account information, whether user-
25 managed or not. Those items that are not identified as user-managed are
not accessible through the user's interface.

-387-

1. Provisioning and Fulfillment

Access requirements have been defined in terms of inbound access to the system and outbound access from the system. Inbound access includes the methods through which a user or a caller may access the system. Outbound
5 access includes the methods through which users are handled by the system in accordance with a preferred embodiment. Internet support exists for both inbound and outbound processing.

The following components may provide inbound access:

- 10 • directlineMCI: 800/8XX;
- MCIMail: 800/8XX, email addresses;
- networkMCI Paging: 800/8XX; and
- internetMCI mail: 800/8XX, POP3 email address.

15 The following components have been identified for outbound access:

- directlineMCI: Dial 1;
- Fax Broadcast: 800/8XX, local;
- MCI Mail: 800/8XX, email address; and
- internetMCI mail: 800/8XX, POP3 email address.

20

G. Traffic Systems

Traffic is supported according to current MCI procedures.

H. Pricing

25 Initially, the features are priced according to the existing pricing structure defined for the underlying components. In addition, taxing and discounting capabilities are supported for the underlying components as they are currently being supported. Discounting is also supported for customers that subscribe to multiple services.

30

-388-

I. Billing

The billing system:

- Supports charges for directlineMCI enhanced services (voicemail, faxmail, both);
- 5 • Supports charges for peak and off-peak rates;
- Supports discounts for multiple services (directlineMCI, networkMCI Business, networkMCI Paging, networkMCI Cellular) which will vary based upon number of services;
- 10 • Supports ability to suppress networkMCI Cellular charges for directlineMCI calls (originating and terminating);
- Supports charges for monthly fees sensitive to directlineMCI usage;
- Supports promotions in the form of free minutes based on directlineMCI usage;
- Supports charges for Personal Home Pages;
- 15 • Supports ability to suppress charges for Personal Home Pages; and
- Supports SCA Pricing.

In one embodiment, the billing system supports the current invoicing procedures that exist for each of the underlying components. In an
20 alternative embodiment, the billing provides a consolidated invoice that includes all of the underlying components. In addition to invoicing, directed billing is supported for all of the underlying components that are currently supporting directed billing.

XVIII.DIRECTLINE MCI

25

The following is a description of the architecture of the directline MCI system, as modified for use with the system. This document covers the general data and call flows in the directlineMCI platform, and documents the network and hardware architecture necessary to support those flows.
30 Billing flows in the downstream systems are covered at a very high level. Order Entry (OE) flows in the upstream systems are covered at a very high

-389-

level. Certain portions of the directlineMCI architecture reuse existing components (e.g. the Audio Response Unit (ARU)). Those portions of the directlineMCI architecture which are new are covered in more detail.

5 A. **Overview**

In addition to billing, order entry, and alarming, the directlineMCI system is made up of three major components, as shown in Figure 43:

- ARU (Audio Response Unit) **502**
- VFP (Voice Fax Platform) **504**
- 10 • DDS (Data Distribution Service) **506**

The subsections below describe each of the major components at a high level.

Figure 43 shows the high-level relationships between the major system components.

15 1. The ARU (Audio Response Unit) **502**

The ARU **502** handles all initial inbound calls for directlineMCI. Some features (such as find me/follow me) are implemented entirely on the ARU. Inbound faxes are tone-detected by the ARU and extended to the VFP **504**. Menuing provided by the ARU can be used to request access to the
20 voicemail/faxmail features, in which case the call is also extended to the VFP.

2. The VFP (Voice Fax Platform) **504**

The VFP provides the menuing for the voicemail/faxmail features as well as outbound fax and voice forwarding and pager notifications. The VFP is also
25 the central data store for the customized subscriber prompts which are played and recorded by the ARU **502**.

3. The DDS (Data Distribution Service) **506**

The DDS is a central data repository for OE profiles and Billing Details Records (BDRs). OE profiles are deposited with DDS, which is responsible

-390-

for distributing the profiles to all of the appropriate systems. DDS **506** collects BDRs and ships them to the downstream billing systems.

B. Rationale

5 The requirement for the directlineMCI service is to integrate a variety of service components into a single service accessed by a single 800 number. A number of these service components had been previously developed on the ISN ARU platform. The services not present in the ARU were mailbox services and fax services. The ARU **502** of the system **500** incorporates a
10 voicemail/faxmail platform purchased from Texas Instruments (TI). Portions of that software are ported to run on DEC Alpha machines for performance, reliability, and scalability. Another requirement for the directlineMCI implementation is integration with the mainstream (existing MCI) billing and order entry systems. The DDS provides the inbound and outbound
15 interfaces between directlineMCI and the mainstream order entry systems.

C. Detail

Figure **43** shows the relationships between the major system components. The OE system **508** generates subscriber profiles which are downloaded via
20 DDS **506** to the ARU **502** and the Voice Fax Platform (VFP) **504**. BDRs generated by the ARU **502** and VFP **504** are fed to the billing systems **510** via DDS **506**. The ARU **502** handles all inbound calls. If faxtone is detected, or if a voicemail/faxmail feature is requested, the call is extended from the ARU **502** to the VFP **504**. For mailbox status (e.g. " You have three
25 messages"), the ARU **502** queries the VFP **504** for status and plays the prompt.

Subscribers' customized prompts are stored on the VFP **504**. When the ARU plays the customized prompt, or records a new prompt, the prompt is
30 accessed on the VFP **504**. Alarms from the ARU **502** and VFP **504** are sent

to the Local Support Element (LSE).

1. Call Flow Architecture **520**

The call flow architecture for directlineMCI is shown in Figure **44**. The top
5 part of the figure shows the network **522** connectivity used to transport the
calls. The bottom part of the figure shows the call direction for different call
types. The subsections below provide the text description to accompany the
figure.

2. Network Connectivity

10 All inbound ISN calls are received at an Automatic Call Distributor (ACD)
524 connected to the MCI network **522**. The Access Control Point (ACP)
receives notice of an inbound call from the Integrated Services Network
Application Processor (ISNAP) **526**, which is the control/data interface to the
15 ACD 524. The Network Audio System (NAS) plays and records voice under
the control of the ACP via a T1 interface to the ACD. In the United States, a
digital multiplexing system is employed in which a first level of multiplexed
transmission, known as T1, combines 24 digitized voice channels over a
four-wire cable (one-pair of wires for "send" signals and one pair of wires for
20 "receive" signals). The conventional bit format on the T1 carrier is known as
DS1 (i.e., first level multiplexed digital service or digital signal format), which
consists of consecutive frames, each frame having 24 PCM voice channels
(or DS0 channels) of eight bits each. Each frame has an additional framing
bit for control purposes, for a total of 193 bits per frame. The T1
25 transmission rate is 8000 frames per second or 1.544 megabits per second
(Mbps). The frames are assembled for T1 transmission using a technique
known as time division multiplexing (TDM), in which each DS0 channel is
assigned one of 24 sequential time slots within a frame, each time slot
containing an 8-bit word.

-392-

Transmission through the network of local, regional and long distance service providers involves sophisticated call processing through various switches and hierarchy of multiplexed carriers. At the pinnacle of conventional high-speed transmission is the synchronous optical network (SONET), which utilizes fiber-optic media and is capable of transmission rates in the gigabit range (in excess of one-billion bits per second). After passing through the network, the higher level multiplexed carriers are demultiplexed ("demuxed") back down to individual DS0 lines, decoded and coupled to individual subscriber telephones.

Typically, multiple signals are multiplexed over a single line. For example, DS3 transmission is typically carried by a coaxial cable and combines twenty-eight DS1 signals at 44.736 Mbps. An OC3 optical fiber carrier, which is at a low level in the optical hierarchy, combines three DS3 signals at 155.52 Mbps, providing a capacity for 2016 individual voice channels in a single fiber-optic cable. SONET transmissions carried by optical fiber are capable of even higher transmission rates.

The NAS/ACP combination is referred to as the ARU **502**. If the ARU **502** determines that a call must be extended to the VFP **504**, it dials out to the VFP **504**. The VFP media servers are connected to the MCI network **522** via T1. Data transfer from the ARU **502** to the VFP **504** is accomplished via is Dual Tone Multi-Frequency (DTMF) on each call.

3. Call Flow

The call scenarios shown in Figure **44** are detailed below. At the start of any of the inbound calls, the ARU **502** has already received the call and performed an application select to determine whether the call is a directlineMCI call or not.

-393-

a) Inbound FAX:

An inbound FAX call is delivered to the ARU **502**. The ARU performs a faxtone detect and extends the call to the VFP **504**. Account number and mode are delivered to the VFP utilizing DTMF signaling.

5

b) Inbound Voice, ARU only:

An inbound voice call is made in either subscriber or guest mode, and only those features which use the ARU **502** are accessed. The ARU determines mode (subscriber or guest). In subscriber mode, the ARU queries the VFP **504** to determine the number of messages. No additional network accesses are made.

10

c) Inbound/Outbound Voice, ARU only:

A call is made to the ARU **502**, and either pager notification or find me/follow me features are accessed. The ARU **502** dials out via the ACD **524** to the outside number.

15

d) Inbound Voice, VFP features:

A call is made to the ARU **502**, and the call is extended to the VFP **504**. Account number and mode (subscriber or guest) are sent to the VFP via DTMF. The guest modes are:

20

1. Deposit voicemail.
2. Deposit fax mail.
3. Collect fax mail.

25 The subscriber modes are:

1. Retrieve or send mail.
2. Maintain broadcast lists.
3. Modify mailbox name recording.

-394-

The VFP **504** continues prompting the user during the VFP session.

e) Outbound Fax/Voice/Pager, VFP only:

For FAX or voice delivery or pager notification, the VFP dials out on the MCI
5 network **522** directly.

f) Reoriginate/Takeback:

While an inbound subscriber call is connected to the VFP **504**, the user
may return to the top level of the ARU **502** directlineMCI menus by pressing
10 the pound key for two seconds. The network **522** takes the call back from
the VFP **504** and reoriginates the call to the ARU **502**.

4. Data Flow Architecture

Figure **45** depicts the primary data flows in the directlineMCI architecture
15 **520**:

OE records (customer profiles) are entered in an upstream system and are
downloaded at **530** to the DDS mainframe **532**. The DDS mainframe
downloads the OE records to the Network Information Distributed Services
(NIDS) servers **534** on the ARU/ACP and the VFP/Executive Server **536**.
20 These downloads are done via the ISN token ring network **538**. On the
executive server **536**, the OE records are stored in the local Executive Server
database (not shown).

BDRs are cut by both the Executive Server **536** and the ACP **540**. These
25 BDRs are stored in an Operator Network Center (ONC) server **542** and are
uploaded to the DDS mainframe **532**. The uploads from the ONC servers
542 to the DDS mainframe are done via the ISN token ring network **538**.

The ARU **502** prompts subscribers with their number of voicemail/faxmail

-395-

messages. The number of messages a subscriber has is obtained from the VFP **504** by the ACP **540** over the ISNAP Ethernet **544**. Note that the ACPs **540** may be at any of the ISN sites.

- 5 The user-recorded ad hoc prompts played by the NAS **546** are stored on the VFP **504** and are played over the network on demand by the NAS **546**. The NFS protocol **548** is used over the ISNAP Local Area Network (LAN) **544** and Wide Area network (WAN) **550**.

10 **D. Voice Fax Platform (VFP) 504 Detailed Architecture**

1. Overview

Figure **46** shows the hardware components of the Voice Fax Portion **504** of the directlineMCI system for the first embodiment. The main components in this system are:

- 15 The TI MultiServe 4000 media server **560**.
The DEC 8200 executive servers **536**.
The Cabletron MMAC+ hubs **562**.
The AlphaStation 200 console manager and terminal servers **564**.
The Bay Networks 5000 hubs **566**.

20

In another embodiment, the Cabletron hubs will be removed from the configuration, and the Bay Networks hubs will then carry all the network traffic.

25 2. Rationale

The TI MultiServe 4000 **560** was selected by MCI for the voicemail/faxmail portion of the directlineMCI platform. The MultiServe 4000 is a fairly slow 68040 machine on a fairly slow Nubus backplane. The 68040/Nubus machines are used by TI as both media servers (T1 interface, DSPs for voice

-396-

and fax) and also for the executive server (database and object storage). Although this hardware is adequate for media server use, it was inadequate as an executive server to serve hundreds or even thousands of gigabytes of voice and fax data and thousands of media server ports. Additionally, there
5 is no clustering (for either performance or redundancy) available for the media server hardware. Thus, the executive server portion of the TI implementation was ported by MCI to run on a DEC Alpha 8200 cluster **536**, described below. This clustering provides both failover and loadsharing (thus scalability).

10 Likewise, the gigabytes that must be moved from the high speed 8200 platforms must be moved across a network to the TI media servers. Cabletron Hubs **562** with both Fiber Distribution Data Interface (FDDI) and switched 10bT connectivity provide the backbone for the implementation. Each media server **560** is attached to a redundant pair of switched Ethernet
15 ports. Because each port is a switched port, each media server gets a dedicated 10Mb of bandwidth to the hub. The 8200 servers **536** each need a large network pipe to serve the many smaller 10Mb Ethernet pipes. For the first embodiment, the FDDI interfaces **568** will be used. However, traffic projections show that the necessary traffic will exceed FDDI capacity by
20 several times, so an embodiment in accordance with a preferred embodiment will use higher speed networking technology such as ATM. The hub **562** configuration is fully redundant.

The AlphaStation 200 workstation **564** is needed for operations support.

25 The AlphaStation 200 provides console management via DEC's Polycenter Console Manager for each of the directlineMCI VFP **504** components. It also runs the DEC Polycenter Performance Analyzer software. The performance analyzer software collects and analyzes data from the 8200s for tuning purposes.

-397-

3. Detail

Figure **47** shows the production installation of the VFP **504** at the production site.

Notes about Figure **47** and its relationship to Figure **46**:

- 5 The DEC Alpha 8200s **536** are in a failover configuration. The center rack is a shared disk array.

- 10 The TI MultiServe 4000 **560** is actually compound of four separate media servers in a single cabinet. The diagrams after this one show each "quadrant" (one of the four media servers in a MultiServe 4000) as a separate entity. Four each of the 16 FGD T1s are connected to each quadrant.

- 15 The AlphaStation 200 workstation **564** and the terminal servers are used to provide console and system management. The Cabletron hubs **562** provide the network between the media servers **560** and the executive servers **536**.

- 20 The Bay Networks hubs **566** provide the network between the VFP 504 and the network routers **569**.

a) Internal Hardware Network

Figure **48** shows the VFP internal hardware/network architecture:

General notes about Figures **47-49**:

- 25 The left DEC 8200 machine **536** is shown with all of its ATM and FDDI connections **570** drawn in. The right DEC 8200 is shown with its Ethernet connections **572** drawn in. In actual deployment, both machines have all of the ATM, FDDI, token ring, and Ethernet connections **570** and **572** shown. The Cabletron hubs **562** show fewer connections into ports than actually occur because each 8200 **536** is drawn with only half its network
- 30 connectivity. Also, only one of the four media servers **560** is shown connected to the Ethernet ports. In fact, there is a transceiver and two

Ethernet connects for each media server.

The Bay Hubs **566** are not shown in Figure **48**. They are shown in Figure **49**, directlineMCI VFP External LAN Network Connectivity.

5

Starting from the top of Figure **48** of the DEC 8200s 536:

The top unit contains three 4GB drives **574** for operating system, swap, etc.

The system CD drive **576** is also located here. This unit is controlled by the Single-Ended Small Computer Systems Interface (SCSI) ("SES" on the

10 diagram) interface **578** from the main system **579**.

The tape stacker **580** is a 140GB tape unit with a single drive and a 10 tape stack. This unit is controlled from a Fast-Wide SCSI ("FWS" on the diagram) interface **582** from the main system **579**.

15

The main system unit **579** utilizes three of five available slots. Slot 1 has the main CPU card **584**. This card has one 300MHz CPU and can be upgraded to two CPUs. Slot 2 has a 512MB memory card **586**. This card can be upgraded to 2GB, or another memory card can be added. System
20 maximum memory is 4GB.

Slots 3 and 4 are empty, but may be used for additional CPU, memory, or I/O boards. Slot 5 has the main I/O card **588**. This card has eight I/O interfaces:

25 One Fast-Wide SCSI interface **582** controls the tape stacker.

Two Fast-Wide SCSI interfaces **590-592** are unused.

The Single-Ended SCSI interface **578** controls the local system drives.

The FDDI interface **594** connects to one of the hubs.

The PCI slot **596** connects to a PCI expansion chassis **598**.

30 One port is a 10baseT Ethernet card **600** that is connected to the corresponding card in the other 8200 **536** via a private thinnet Ethernet. This network is required for one of the system failover heartbeats.

-399-

An embodiment utilizes nine of the ten available slots in the PCI/EISA expansion chassis **598**. Slots 1 and 2 have disk adapters **602**. Each disk adapter **602** is connected to a RAID disk controller **604** that has another
5 disk controller **604** (on the other machine) chained, which in turn is connected to a disk controller **604** on that machine. Thus, each of the 8200 machines **536** has two disk controllers **604** attached off of each disk adapter **602**. This is the primary clustering mechanism, since either machine can control all of the disks located in Figure **48** beneath the PCI
10 chassis **598**. Slot 3 has a Prestoserve board **606**. This is a Network File Server (NFS) accelerator.

Slot 4 has an FDDI board **608**. This FDDI connection is made to the hub other than the FDDI connection made from main slot 5 above.

15 Slots 5 and 6 have ATM boards **610**. It has a 10baseT Ethernet card **612** that is connected to the corresponding card in the other 8200 **536** via a private thinnet Ethernet. This network is required for one of the system failover heartbeats. Slot 10 is empty.

20 The two units beneath the PCI chassis are Redundant Array of Inexpensive Disks (RAID) disk controllers **604**. Each disk controller **604** is on a SCSI chain with two disk controllers **604** in the middle and a disk adapter **602** (one per machine) on each end. Thus there are two chains, each with two disk controllers **604** and two disk adapters **602**. This is the connectivity to
25 the main system **579**. Each disk controller **604** supports six single-ended SCSI chains. In this configuration, each of the two chains has one disk controller with two SES connections, and one disk controller with three connections. Each chain has five sets **614** (or "drawers") of disk drives as pictured in the center rack. Note the redundant power supply in the drawer
30 with the RAID Disk Controller.

The Cabletron MMAC+ hubs **562** (Figure **47**) are configured in a redundant

-400-

- pair. Both the 8200s **536** and the TI media servers **560** connect to both hubs **562**, and the two hubs **562** are also connected to each other. Starting from the left side of the hubs: The FDDI concentrator card **616** provides an eight port FDDI ring. Each 8200 has one connection into the FDDI card
- 5 **616** on each hub **562**. The 24 port Ethernet card **618** provides connectivity to the TI media servers **560**. Each media server **560** connects into one Ethernet port **618** on each hub. There are eight empty slots **620** in each hub which can be used for additional FDDI, ATM, or Ethernet expansion.
- 10 There are four TI media servers **560** mounted in a single rack called a "MultiServe 4000". Each media server in the rack is identical. Starting from the top unit, and then proceeding left to right for the main slots: The top unit **622** is a drawer that contains two 1GB disk drives, and a
- 15 removable/hot-insertable tape drive. There are two tape drives that can be shared among the four media servers. The left seven boards **624** labeled "DSP xxx" are TI MPB boards which can each support six incoming or fifteen outgoing channels, as labeled. These boards **624** are grouped together into three sets. There is a right group of three boards, a middle group of three boards, and a single board on the left. Each group has one T1. The T1
- 20 terminates at the interface marked "T1M". This is the master T1 interface. T1 channels may be shared by the set of boards delimited by the master/slave T1 boards, and chained together by the bridge modules. The rightmost board **626** is the main CPU/IO board. This board supports an SCSI interface **628** to the disk drawer, an Ethernet connection **630** to a
- 25 special transceiver **632**, and a serial port for the console (not shown).

The transceiver **632** to the right of the CPU/IO board connects to Ethernet ports on each of the two main hubs **562**. The transceiver senses if one of its Ethernet connections has failed, and routes traffic to the other port.

-401-

b) External Hardware/Network Connections

Figure **49** shows the hardware and network connections from the VFP **504** to the external network. Notes about Figure **49**: Each 8200 **536** is connected onto the ISN token ring **640** through the Bay Hubs for DDS access over SNA and BDR access over IP. A pair of terminal servers **642** has a connection to the console port of each machine and hub. A DEC AlphaStation 200 **564** runs console manager software to access the ports connected to the terminal servers **642**. The DECNIS routers are all on an FDDI ring **568** (Figure **46**), connected between the Bay Hubs **566** and the two DEC 8200s **536**.

The Bay Hubs **566** connect the VFP system **504** to the external network through the seven routers **644** shown.

E. Voice Distribution Detailed Architecture**1. Overview**

Voice Distribution refers to the portion of the architecture in which the NAS **546** (Figure **45**) reads and writes the subscriber's ad hoc prompts across the LAN or WAN from/to the VFP **504** using the NFS protocol.

2. Rationale

In one embodiment, voice distribution is implemented by placing a server at each ISN site and replicating the data via complex batch processes from each server to every other server.

The "Large Object Management" (LOM) project defines a network-based approach. It was decided to use the directlineMCI VFP **504** as the network-based central object store for the NAS **546** to read and write customer prompts.

-402-

Figure **50** shows a network architecture to support Voice distribution traffic in accordance with a preferred embodiment. Figure **52A** depicts a configuration of the Data Management Zone **5105** of the present invention.

5 The Data Management Zone (DMZ) is a firewall between Internet dial-in platforms (although not the actual Internet itself) and the ISN production networks. Its purpose is to provide dial-in access to data for ISN customers while maintaining security for the ISN network as well as privacy and integrity of customer data in a production ISN network.

10

The DMZ permits a customer to receive periodically generated data, such as DDS data down feeds from a mainframe database. Such data is periodically extracted from the database and placed in a user account directory on a secure File Transfer Protocol (FTP) host for subsequent retrieval by a

15 customer.

Data access for customers is through dedicated ports at dial-in gateways, which are owned, operated and maintained by the Internet provider. Dial-in user authentication is through the use one time passwords via secure

20 identification cards, as is more fully described below. The cards are distributed and administered by Internet provider personnel.

The DMZ provides a screened subnet firewall that uses a packet filtering router to screen traffic from the outside unsecured network and the internal

25 private network. Only selected packets are authorized through the router, and other packets are blocked. The use of multiple firewalling techniques ensures that no single point of failure or error in DMZ configuration puts the ISN production network at risk.

30 The DMZ **5105** is intended to conform to several security standards. First, individuals who are not authorized employees cannot be allowed access to internal production networks. Therefore IP connectivity through the

-403-

gateway is not allowed. Second, access and use of DMZ services is restricted to authenticated and authorized users for specific purposes. Therefore all other utilities and services normally found on a general purpose machine are disabled. Third, use of DMZ services and facilities must be carefully
5 monitored to detect problems encountered by authorized users and to detect potentially fraudulent activity.

The centerpiece of the DMZ is the DMZ Bastion host **5110**. Bastion host **5110** runs an FTP server daemon that implements a modified FTP protocol,
10 as will be described in further detail below. Bastion host **5110** is a highly secured machine used as the interface to the outside world. Bastion host **5110** allows only restricted access from the outside world. It typically acts as an application-level gateway to interior hosts in ISN **5115**, to which it provides access via proxy services. Generally, critical information is not
15 placed on Bastion host **5110**, so that, even if the host is compromised, no access is made to critical data without additional integrity compromise at the ISN **5115**.

Bastion host **5110** is connected to both interior and exterior users as shown
20 in Figure **52A**. Bastion host **5115** may be a UNIX-based computer such as an IBM RS/6000 model 580 running the AIX operating system.

An interior user is a user connected to the ISN production token ring **5115**. Token ring **5115** is connected to an interior packet filter **5120** such as a
25 Cisco model 4500 modular router. Packet filter **5120** is connected to token ring LAN **5125**, which in turn is connected to bastion host **5110**. Token ring LAN **5125** is a dedicated token ring that is isolated from all components other than bastion host **5110** and interior packet filter **5120**, thereby preventing any access to bastion host **5110** through token ring LAN **5125**
30 except as allowed by packet filter **5120**.

Exterior users connect through exterior packet filter **5130**, such as a Cisco

-404-

model 4500 modular router. Packet filter **5130** is connected to bastion host **5110** through an isolated Ethernet LAN segment **5135**. Ethernet LAN segment **5135** is a dedicated segment that is isolated from all components other than bastion host **5110** and exterior packet filter **5130**. Because of the configuration, no user can access bastion host **5110** except through interior packet filter **5120** or exterior packet filter **5130**.

Figure **52A** depicts the DMZ **5105** in connection with dial-in environment **5205**. In dial-in environment **5205**, the customer PC **5210** is connected to public switched telephone network (PSTN) **5220** through the use of modem **5215**. Modem bank **5230** assigns a modem to answer incoming calls from PSTN **5220**. Modem bank **5230** comprises a set of high-speed modems **5233** such as U.S Robotics V.34 Kbps modems. Incoming calls are authenticated by authentication server **5235**. Authentication server **5235** may be implemented using a server such as the Radius/Keystone server running on a Sun Sparcstation model 20.

The Bastion host **5110** resides within a firewall, but is logically outside both the ISN **5115** and the gateway site **5205**.

Following authentication, the selected modem **5233** is connected to incoming call router **5240** using Point-to-Point Protocol (PPP). PPP is a protocol that provides a standard method of transporting multi-protocol datagrams over point-to-point links. PPP is designed for simple links that transport packets between two peers. These links provide full-duplex simultaneous bi-directional operation, and are assumed to deliver packets in order. PPP provides a common solution for easy connection of a wide variety of hosts, bridges and routers). PPP is fully described in *RFC 1661: The Point-to-Point Protocol (PPP)*, W. Simpson, Ed. (1994) ("RFC 1661"), the disclosure of which is hereby incorporated by reference.

Incoming call router **5240** selectively routes incoming requests to the

-405-

exterior packet filter **5130** of DMZ **5105** over a communications link such as T1 line **5250**, which is connected to exterior packet filter **5130** via a channel service unit (not shown). Incoming call router **5240** may be implemented using, for example, a Cisco 7000 series multiprotocol router.

- 5 Incoming call router **5240** is optionally connected to Internet **5280**. However, router **5240** is configured to block traffic from Internet **5280** to Exterior packet filter **5130**, and to block traffic from exterior packet filter **5130** to Internet **5280**, thereby disallowing access to DMZ **5105** from Internet **5280**.

10

Bastion host **5110** runs a File Transfer Protocol (FTP) server daemon that implements a modified FTP protocol based on release 2.2 of the *wu-ftpd* FTP daemon, from Washington University. Except as noted herein, the FTP protocol is compliant with *RFC 765: File Transfer Protocol*, by J. Postel (June 15 1980) ("RFC 765"), the disclosure of which is hereby incorporated by reference. RFC 765 describes a known protocol for transmission of files using a TCP/IP-based telnet connection, in which the server responds to user-initiated commands to send or receive files, or to provide status information. The DMZ FTP implementation excludes the *send* command (which is used to send a file from a remote user to an FTP server, and any 20 other FTP command that transfers files to the FTP host. A restricted subset of commands including the *get* (or *recv*), *help*, *ls*, and *quit* commands are supported.

- 25 The *get* command is used to transfer a file from host server **5110** to remote user **5210**. The *recv* command is a synonym for *get*. The *help* command provides terse online documentation for the commands supported by host server **5110**. The *ls* command provides a list of the files in the current directory of the server, or of a directory specified by the user. The *quit* 30 command terminates an FTP session. Optionally, the *cd* command, which specifies a named directory as the current directory, and the *pwd* command, to display the name of the current directory, may be implemented.

-406-

By disallowing *send* and other commands that transfer files to the server, a potential intruder is prevented from transferring a "Trojan horse" type of computer program that may be used to compromise system security. As an additional benefit, the unidirectional data flow prevents a user from inadvertently deleting or overwriting one of his files resident on the Bastion server.

When the FTP daemon initiates a user session, it uses the UNIX *chroot(2)* service to specify the root of the user's directory tree as the apparent root of the filesystem that the user sees. This restricts the user from visibility to UNIX system directories such as */etc* and */bin*, and from visibility to other users' directories, while permitting the desired visibility and access to the files within the user's own directory tree. To further assure a secured environment, the FTP daemon executes at the user-id ("uid") of the user level, rather than as *root*, and allows access only to authorized users communicating from a set of predetermined IP addresses known to be authorized. In particular, the standard non-authenticated accounts of *anonymous* and *guest* are disabled.

In order to further secure Bastion server **5110**, a number of daemons that are ordinarily started by the UNIX Internet server process *inetd* are disabled.

The disabled daemons are those that are either not needed for Bastion server operation, or that are known to have security exposures. These daemons include *rcp*, *rlogin*, *rlogind*, *rsh*, *rshd*, *tftp*, and *tftpd*. These daemons are disabled by removing or commenting out their entries in the AIX */etc/inetd.conf* file. The */etc/inetd.conf* file provides a list of servers that are invoked by *inetd* when it receives an Internet request over a socket.

By removing or commenting out the corresponding entry, the daemon is prevented from executing in response to a received request.

As a further assurance of security a number of daemons and utilities are

-407-

disallowed from execution by changing their associated file permissions to mark them as non-executable (e.g., having a file mode of 000). This is performed by a DMZ Utility Disabler (DUD) routine that executes at boot time. The DUD routine marks as non-executable the above-identified files
5 (*rcp*, *rlogin*, *rlogind*, *rsh*, *rshd*, *tftp*, and *tftpd*), as well as a number of other daemons and utilities not ordinarily invoked by *inetd*. This set of daemons and utilities includes *sendmail*, *gated*, *routed*, *fingerd*, *rexecd*, *uucpd*, *bootpd*, and *talkd*. In addition, DUD disables the *telnet* and *ftp* clients to prevent an intruder from executing those clients to access an interior host in the event
10 of a break-in. The *telnet* and *ftp* clients may be temporarily marked as executable during system maintenance activities.

Bastion host **5110** has IP forwarding disabled. This ensures that IP traffic cannot cross the DMZ isolated subnet **5115** by using Bastion host **5110** as
15 a router.

The limited level of ftp service provided by Bastion server **5110** provides a secure ftp session but makes it difficult to perform typical system maintenance. In order to perform system maintenance, maintenance
20 personnel must connect to Bastion host **5110** from an interior host within ISN **5115** using a telnet client. The FTP client program in Bastion is then changed from non-executable (e.g., 000) to executable (e.g., 400), using the AIX *chmod* command. Maintenance personnel may then execute the ftp client program to connect to a desired host on ISN **5115**. During this
25 procedure, control of transfers is therefore from within Bastion host **5110** via the FTP client program executing within that host, rather than from a client outside of the host. At the end of a maintenance session the FTP session is terminated, and the *chmod* command is executed again to revert the ftp client program to a non-executable state (e.g., 000), after which the
30 ISN-initiated telnet session may be terminated.

To provide logging, Bastion server **5110** implements a TCP daemon wrapper,

-408-

such as the TCPwrappers suite from Wietse Venema. The TCP wrapper directs *inetd* to run a small wrapper program rather than the named daemon. The wrapper program logs the client host name or address and performs some additional checks, then executes the desired server program on behalf of *inetd*. After termination of the server program, the wrapper is removed from memory. The wrapper programs have no interaction with the client user or with the client process, and do not interact with the server application. This provides two major advantages. First, the wrappers are application-independent, so that the same program can protect many kinds of network services. Second, the lack of interaction means that the wrappers are invisible from outside.

The wrapper programs are active only when the initial contact between client and server is established. Therefore, there is no added overhead in the client-server session after the wrapper has performed its logging functions. The wrapper programs send their logging information to the syslog daemon, *syslogd*. The disposition of the wrapper logs is determined by the syslog configuration file, usually */etc/syslog.conf*.

Dial-in access is provided through dial-in environment **5105**. The use of authentication server **5235** provides for authentication of users to prevent access from users that are not authorized to access the DMZ. The authentication method implemented uses a one-time password scheme. All internal systems and network elements are protected with one-time password generator token cards, such as the SecurID secure identification token cards produced by Security Dynamics, using an internally developed authentication client/server mechanism called Keystone. Keystone clients are installed on each element that receive authentication requests from users. Those requests are then securely submitted to the Keystone Servers deployed throughout the network.

Each user is assigned a credit card sized secure identification card with a

-409-

liquid crystal display on the front. The display displays a pseudo-randomly generated six-digit number that changes every 60 seconds. For an employee to gain access to a Keystone protected system, the user must enter their individually assigned PIN number followed by the number currently

5 displayed on the secure identification card. Such authentication prevents unauthorized access that employ the use of programs that attempt to "sniff" or intercept passwords, or Trojan horse programs designed to capture passwords from users.

- 10 Authentication information collected by the Keystone clients is encrypted with an RSA and DES encryption key, and is dispatched to one of many Keystone Servers. The Keystone Servers evaluates the information to verify the user's PIN and the access code that should be displayed on that user's card at that moment. After the system verifies that both factors for that user
- 15 where entered correctly, the authorized user is granted access to the system, or resource requested.

- In order to assure security from the point of entry of the external network, no external gateway machine has a general access account and all provide
- 20 controlled access. Each gateway machine ensures that all gateway services generate logging information, and each external gateway machine maintains an audit trail of connections to the gateway. All of the external gateway machines have all non-essential services disconnected.

- 25 The authentication server **5235** serves as a front end to all remote access dial up, and is programmed to disallow pass-through. All network authentication mechanisms provide for logging of unsuccessful access attempts. Preferably, the logs generated are reviewed daily by designated security personnel.

30

Figure **53** depicts a flow diagram showing the fax tone detection methodology. In step **5305**, the fax tone detection system allocates a null

-410-

linked-list; that is, a linked list having no entries. In step **5310**, the fax tone detection system starts the asynchronous routine `auCheckForFaxAsync` **5315**. The `auCheckForFaxAsync` routine **5315** is an asynchronous program that executes concurrently with the main line program, and rather than
5 synchronously returning control to the calling program. The `auCheckForFax` routine evaluates the tone of the incoming call to see whether the call is originated by a facsimile machine, and generates an `auCheckForFax` response **5318** if and when a facsimile tone is detected.

10 After starting `auCheckForFaxAsync` routine **5315**, control proceeds to step **5320**. In step **5320**, the fax tone detection system adds an entry to the linked list allocated in step **5305**. The added entry represents a unique identifier associated with the message being processed. In step **5330**, the fax tone detection system starts the asynchronous routine `auPlayFileAsync`
15 **5335**. The `auPlayFileAsync` routine **5335** is an asynchronous program that executes concurrently with the main line program, rather than synchronously returning control to the calling program. The `auPlayFileAsync` routine **5335** accesses previously stored digitally recorded sound files and plays them to the originating caller. The sound files played
20 may be used, for example, to instruct the originating caller on sequences of key presses that may be used to perform particular functions, e.g., to record a message, to retrieve a list of previously recorded messages, etc.

In step **5340**, the fax tone detection system starts the asynchronous routine
25 `auInputDataAsync` **5340**. The `auInputDataAsync` routine **5340** is an asynchronous program that executes concurrently with the main line program, rather than synchronously returning control to the calling program. The `auInputDataAsync` routine **5340** monitors the originating call to detect key presses by the user, in order to invoke the routines to execute
30 the tasks associated with a particular key press sequence.

As has been noted, the `auCheckForFaxAsync` routine **5315** executes

-411-

concurrently with the main program, and generates a auCheckForFax response **5318** if and when a facsimile tone is detected. In step **5350**, the fax tone detection system checks to see whether an auCheckForFax response **5318** response has been received. If a response has been received,
5 this indicates that the originating call is a facsimile transmission, and the fax tone detection system extends the incoming call to Voice/Fax processor (VFP) **5380**. If no auCheckForFax response **5318** is received within a predetermined time (e.g., 7 seconds), the fax tone detection system concludes that the originator of the call is not a facsimile device, and
10 terminates the auCheckForFaxAsync routine **5315**. In an implementation, it may be preferable to implement this check through an asynchronous interruption-handling process. In such an implementation, an execution-time routine may be set up to gain control when an auCheckForFax response **5318** event occurs. This may be implemented using, for example,
15 the C++ *catch* construct to define an exception handler to handle an auCheckForFax response **5318** event.

Following the decision in step **5350**, the fax tone detection system in step **5360** waits for the next incoming call.

20

Figures **54A** through **54E** depict a flow diagram showing the VFP Completion process for fax and voice mailboxes. As depicted in Figure **54A**, the VFP completion routine in step **5401** searches the database for a record corresponding to the addressed mailbox. In step **5405**, the VFP completion
25 routine checks to see if a mailbox record was successfully retrieved. If no mailbox record was found, in step **5407**, the VFP completion routine generates a VCS alarm indicating that the desired mailbox record was not found. Because the mailbox record was not found, the VFP completion processor will be unable to test the attributes of the mailbox address.
30 However, regardless of whether the mailbox record is found, control proceeds to step **5409**. In step **5409**, the VFP completion processor tests the contents of the mailbox record, if any, to determine whether the

-412-

addressed mailbox is full. If the addressed mailbox is full, in step **5410**, the VFP completion routine plays an error message indicating that the addressed mailbox is at capacity and is unable to store additional messages, and exits in step **5412**.

5

In step **5414**, the VFP completion processor obtains the mode of the VFP call. The mode is derived from the dial string provided by the originating caller, and is stored in the enCurrentNum field of the pstCall1State structure. The dial string has the following format:

10

```
{
    char  number[10];      /* 10-digit 8xx number dialed by user
*/
    char  asterisk;        /* constant '*' */
15    char  mode;          /* 1-byte mode */
    char  octothorp;      /* constant '#' */
}
```

The mode has one of the following values:

20

- 1 guest voicemail
- 2 guest fax with voice annotation
- 3 guest fax without voice annotation
- 4 user voice/fax retrieval
- 25 5 user list maintenance
- 6 user recording of mailbox

30

In step **5416**, the VFP completion processor retrieves the route number associated with the addressed mailbox from the database. In step **5418**, the route number is passed to the SIS layer.

As depicted in Figure **54B**, execution continues with step **5420**. In step

5420, the VFP completion processor initialized an answer supervision flag that is used to determine whether the VFP is accepting transfer of the call. In step **5422**, the VFP completion processor calls the SisCollectCall routine to process the call. If the call is unsuccessful, Step **5424** causes the
5 SisCollectCall invocation of step **5422** to be repeated up to a predetermined number of retries.

In step **5426**, the VFP completion processor obtains a predetermined timer expiration value from the otto.cfg file. The timer expiration value is set to
10 the amount of time in which, if an answer is not received, the VFP completion processor may conclude that the VFP is not currently reachable. In step **5428**, the VFP completion processor sets the timer according to the value from step **5426**. In step **5430**, the VFP completion processor check to see whether answer supervision occurred prior to the expiration of the timer
15 set in step **5424**. If so, control proceeds to step **5430** to transfer control to the VFP.

Figure **54C** depicts the operation of transferring control to the VFP in response to an affirmative decision in step **5430**. In step **5440**, any pending
20 timers set in step **5428** are canceled. In step **5442**, the VFP completion processor calls routine sisOnHoldTerm() to put the VFP on hold. In step **5444**, the VFP completion processor calls routine sisOffHoldOrig() to take the originating call off hold.

25 In step **5446**, the VFP completion processor plays a previously stored digitally recorded sound file, instructing the originating caller to wait during the process of transferring the call to the VFP. In step **5448**, the VFP completion processor calls routine sisOnHoldOrig() to put the originating call back on hold. In step **5450**, the VFP completion processor calls routine
30 sisOffHoldTerm to take the VFP off hold. In step **5452**, the VFP completion processor calls the auPlayDigits routine, passing to it as a parameter, a string comprising the addressed mailbox number, an asterisk (*) to indicate

-414-

a field separation, the mode, and an octothorp ('#') to indicate the end of the command string.

In step **5454**, the VFP completion processor obtains a timeout value
5 AckTimeout and an interdigit delay value from the otto.cfg file. The
AckTimeout value is used to determine the amount of time before the VFP
completion processor determines that no response is forthcoming from the
VFP. The interdigit delay value is used to time the delays between audio
signals sent that represent telephone keypad presses. In step **5456**, the
10 VFP completion processor calls the InputData routine to obtain a response
from the VFP.

Following steps **5440** through **5456**, or following a negative decision in step
5430, control proceeds to step **5460**, as shown in Figure **54D**. In step **5460**,
15 the VFP completion processor requests a response from the VFP. In step
5462, the VFP completion processor waits for the VFP response or for a
timer set in step **5428** to expire. In step **5464**, if the VFP has responded,
the VFP completion processor proceeds to step **5446**.

20 In step **5446**, the VFP completion system checks the VFP response and
writes the appropriate BDR term status record. The response indicates the
acknowledgment from the TI platform. A response of '00' indicates success,
and the VFP completion processor writes a BDR_STAT_NORMAL indicator.
A response of '01' indicates the VFP did not receive the key to the addressed
25 mailbox, and the VFP completion processor writes a
BDR_STAT_DLINE_TI_NO_DIGITS indicator. A response of '02' indicates that
the VFP timed out while collecting the key, and the VFP completion
processor writes a BDR_STAT_DLINE_TI_FORMAT indicator. A response of
'03' indicates that the addressed mailbox was not found, and the VFP
30 completion processor writes a BDR_STAT_DLINE_TI_MAILBOX indicator. If
no response was received, a BDR_STAT_DLINE_TI_NO_RSP indicator is
written. Following the BDR indicator, control proceeds to step **5480** as

-415-

shown in Figure **54E**.

If no answer was received from the VFP, the timer set in step **5428** has expired, and control passes to step **5468**. In step **5468** the VFP completion processor gives a VCS alarm indicating that the VFP did not answer. In step **5470**, the VFP completion processor calls routine `sisReleaseTerm()` to disconnect the call to the VFP. In step **5472**, the VCS completion processor calls routine `sisOffHoldOrig` to take the originating call off of hold. In step **5474**, the VFP completion processor calls `tiCancelTimers` to cancel all outstanding timers that have not yet been canceled. In step **5476**, the VFP completion processor plays a previously stored digitally recorded sound file, reporting to the originating caller that the VFP completion processor was unable to connect to the VFP.

After either step **5476** or step **5466** (depending on the decision in step **5464**), control proceeds to step **5480**, as shown in Figure **54E**. In step **5480**, the VFP completion processor checks to see if the originating caller is a subscribed user. If so, control passes to step **5482**. In step **5484**, the VFP completion processor checks to see if the originating caller is a guest user. If so, control passes to step **5482**. Step **5482** then returns the originating caller to the menu from which the caller initiated the VFP request. If the originating caller is neither a subscribed user nor a guest, control passes to step **5486**. In step **5486**, the originating caller is assumed to be a fax call, and the call is disconnected.

Figures **55A** and **55B** depict the operation of the Pager Termination processor. In step **5510**, the pager termination processor calls the `GetCallback` routine to obtain the telephone number that will be used to identify the caller, and that will be displayed on the paging device to identify the number to be called back by the pager subscriber. The `GetCallback` routine is describe in detail below with respect to Figure **56**.

-416-

In step **5515**, the pager termination processor checks to see if a telephone number was returned by the GetCallback. If no number was returned, in step **5520** the pager termination processor indicates that the call should be ended, and in step **5522** provides the caller with a menu to select another
5 service.

If a number was returned, the addressed pagers PIN is obtained from the database in step **5530**. The pager termination processor constructs a pager dial string comprising the pager PIN retrieved in step **5530** and the callback
10 number obtained in step **5510**. In step **5532**, the pager termination processor obtains the pager's type and routing information is obtained from the database. In step **5534**, the pager termination processor checks the configuration file to obtain a pager parse string that defines the parameters for pagers of the type addressed. In step **5536**, the pager termination
15 processor checks to see whether the requested pager parse string was successfully retrieved. If not, in step **5538** the pager termination processor indicates that the page could not be performed by setting the BDR term status to BDR_STAT_PAGER_NOT_FOUND, and in step **5540** provides the caller with a menu to select another service.

20 If the pager parse string was successfully retrieved, the pager termination processor proceeds to step **5550** as shown in Figure **55B**. In step **5550**, the pager termination processor calls the pager subsystem, passing to it the route number, the dial string, and the pager parse string. In step **5552**, the
25 pager termination processor checks the return code from the pager subsystem. If the page was successfully completed, the pager termination processor, in step **5554** plays a digitally prerecorded message to the caller, informing the caller that the page has been successfully sent. In step **5556** the enEndCallStatus field is updated to mark the pager call complete. In
30 step **5558**, the transfer status is marked as blank, indicating that there is no need to transfer the caller, and in step **5560**, the pager termination processor presents the user with a menu permitting it to select another

service or to end the call.

If the page was not successfully completed, the pager termination processor checks in step **5570** whether the caller had disconnected during the page attempt. If the caller had disconnected, the pager termination processor in step **5575** checks to see whether the page had been sent prior to the disconnection. If the page was sent despite the disconnect, the pager termination processor in step **5580** indicates a normal ending to the page request in step **5580** and sets the status as complete in step **5582**. In step **5584**, the pager termination processor presents the user with a menu permitting it to select another service or to end the call.

If the page was not sent the pager termination processor indicates an abnormal ending to the page request in step **5586** and indicates a caller disconnect in step **5588**. In step **5590**, the pager termination processor presents the user with a menu permitting it to select another service or to end the call.

If the caller has not disconnected, the pager termination processor sets a code indicating the reason for the failure in step **5572**. The failure types include BDR_STAT_PAGER_ROUTE_NUM (for an invalid route number); BDR_STAT_PAGER_CRIT_ERROR (for a failure in the originating call); BDR_STAT_PAGER_TIMEOUT (for the failure of the pager to acknowledge the call within a predetermined timeout time interval); BDR_STAT_PAGER_DIGITS_HOLD (for the failure of the pager subsystem to play the digits corresponding to the pager address); BDR_STAT_PAGER_DISC (for a premature disconnect of the paging subsystem); and BDR_STAT_PAGER_NOT_FOUND (for an invalid parse string).

In step **5592** the pager termination processor posts the error code selected in step **5572** to the BDR. In step **5582**, the pager termination processor

-418-

plays a prerecorded digital sound file indicating that the page could not be sent. In step **5595** the enEndCallStatus field is updated to mark the pager call complete. In step **5597**, the transfer status is marked as blank, indicating that there is no need to transfer the caller, and in step **5599**, the pager termination processor presents the user with a menu permitting it to select another service or to end the call.

Figure **56** depicts the GetCallback routine called from the pager termination processor in step **5510**. In step **5610** the GetCallback routine obtains constants that define the applicable start and interdigit delays from the otto.cfg file. In step **5615**, the GetCallback routine plays a prerecorded digital sound file prompting the caller to provide a callback telephone number, by pressing the applicable keypad keys, followed by an octothorp ('#'). In step **5620**, the GetCallback routine reads the number entered by the caller. In step **5625** the data received is placed in the BDR. In step **5630**, the GetCallback routine checks to see if the number entered was terminated by a '#' character. If so, the GetCallback routine returns success in step **5635**. If not, the GetCallback routine, in step **5640**, sees if the retry count has been exceeded. If the retry count has not been exceeded, execution repeats from step **5615**. If the retry count has been exceeded, in step **5650**, the GetCallback routine plays a prerecorded digital message indicating that the number was not successfully received, and in step **5660** returns an error condition to the calling program.

The following description sets forth a user interface for user-management of directlineMCI profile items currently accessed via ARU (DTMF) and Customer Service. These items include:

- Σ (De)Activate Account
- Σ Find-Me Routing
- 30 - Schedules
- 3-Number Sequence
- First, Second, Third Numbers and Ring-No-Answer Timeouts

-419-

- Σ Pager On/Off
- Σ Override Routing
- Σ Final (Alternate) Routing
- Σ Caller Screening
- 5 Σ Pager Notification of Voicemail Messages
- Σ Pager Notification of Faxmail Messages
- Σ Speed Dial Numbers

10 The following table lists the fields that the directlineMCI customer is able to update via DTMF. This list does not include all fields in the service, only those that are used by the directlineMCI application.

Field Name
800# + PIN
Primary Termination
Primary Time-out Value
Secondary Termination
SecondaryTime-out Value
Tertiary Termination
TertiaryTime-out Value
Override Routing
Override Time-out Value
Alternate Routing
Alternate Time-out Value

-420-

PIN_Flags, specifically:

Bit 10

Schedule 1

Bit 11

Schedule 2

Bit 15 Page

on Vmail

Bit 16 Page

on Fax

State_Flags,
specifically:

Bit 3 Account

Available

Bit 13 Pager

On/Off

Bit 14 Find-Me

On/Off

Bit 15 Voicemail

On/Off

Bit 16 Fax

On/Off

Call Screening State

Default Fax Number

Speed Dial #1

Speed Dial #2

Speed Dial #3

Speed Dial #4

Speed Dial #5

Speed Dial #6

Speed Dial #7

Speed Dial #8

Speed Dial #9

A user will access his directlineMCI profile via
http://www.mci.services.com/directline. Upon entry of a valid Account ID
and Passcode, the user's Routing Screen will be presented. The user may
5 click on tabs to move from one screen to another. If a user returns to a
screens that's been updated during that session, the screen will be
displayed as it was when he last left it, i.e. any updates he's submitted will
be reflected in the data. If, however, a user logs off, or times out, when next
he logs into his profile management screens, the data displayed will be from
10 a new query into the 800PIN_1Call database. Updates made within the last
15 minutes may not have reached the NIDS databases serving the Web
Server, so the data may not reflect any recent updates.

The following items will appear in the index frame, and will act as links to
15 their associated Web screens. When a user 'clicks' on one of these items,
the associated screen will be displayed in the text frame.

Call Routing
Guest Menu
20 Override Routing
Speed Dial Numbers
Voicemail
Faxmail
Call Screening

25

In addition, a LOGOFF button will appear at the bottom of the index frame.
Clicking on this button will result in immediate token expiration, and the
user will be returned to the login screen.

F. Login Screen

30 Figure **57** shows a user login screen **700** for access to online profile

-422-

management.

directlineMCI Number 702

The account ID will be the directlineMCI customer's 10-digit access number, of the format 8xx xxx xxxx. This number, concatenated with a PIN of '0000',
5 will be the key into the 1Call database, which contains the customer profile data.

The user will not be allowed a successful login if the Program flag (PIN flag 4) is set to 'N'. If a login attempt is made on such an account, the Login Error
10 screen will be displayed.

Passcode 704

The passcode will be the same as that used to access user options via the ARU interface. It is a six-character numeric string. The user's entry will not
15 be echoed in this field; an asterisk (*) will be displayed for each character entered.

Status message

directlineMCI Number: "Enter your directlineMCI number."
20 Passcode: "Enter your passcode."

G. Call Routing Screen

Figure 58 shows a call routing screen 710, used to set or change a user's call routing instructions.
25

"Accept Calls" Section 712

The user can specify whether calls are accepted at 712 on her account by selecting the appropriate radio button 714 or 716. These buttons correspond directly to the Account Available flag (State flags, bit 3) in the
30 customer's directline record:

-423-

Radio Buttons	Account Available flag
Accept Calls	Y
Do Not Accept Calls	N

“Choose from the selections below” Section 718

The user specifies whether the guest caller should receive a Guest Menu, or Override Routing treatment. This selection will indicate whether the data in the Guest Menu or Override Routing screen is applicable.

The customer's Override Termination will be populated as follows, according to the user's selection:

'Offer Guests...' Radio Buttons	Override Termination
Guest Menu	00
No Menu - Override Routing	08* (default voicemail)

“When I cannot be reached...” Section 720

A user specifies call treatment for those calls for which he was unable to be reached . The Alternate Termination in the customer record is updated as follows:

Radio Buttons	Alternate Termination
Voicemail	08
Pager	07
Voicemail or Pager - Caller Choice	09